International Journal of Scientific & Engineering Research Volume 9, Issue 4, April-2018
ISSN 2229-5518



# Intrusion Detection System using DM Tools

[1]K.Mohanapriya, [2]Dr.M.Savitha Devi.

**Abstract—**we use internet for all of our works (such as e-commerce, bank transactions, healthcare) and also entertainments (chatand post our views in social networks).While using internet, Security and Privacy are prime concern for safe process. Integrity, Authentication, confidentiality and availability are provides Security to access and transfer our data. But Intrusion is main threat for the above Security measures and privacy.

To overcome this, Intrusion Detection System has been used for Network Protection existing Intrusion Detection Systems (IDS) are limited and sometimes they find correct detection of security attacks and in many cases, they fail to detect or misfire when nothing wrong in the Network. We propose Intrusion Detection Systems that have the combination of Data Mining (DM) Techniques and Network Behavior Analysis (NBA) on Network. The Proposed system is works as follows; the suspicious activities and Network Traffic events are collected from Computer Network and then transmit these data to Network Behavior Analysis Intrusion Detection unit and Data Mining-Intrusion Detection unit. Finally Managerial Decision Maker unit that analyzes Intrusion results evaluates system performance, take decisions on detected Intrusions, checks for False Positives and False Negatives, control system operations, generate a performance report and decides if any changes/updates are needed. In some cases the IDS may take action such as blocking the user or source IP address from accessing the Network.

**Keywords—** Security, Attacks, Intrusion.

## 1 Introduction

Generally the following security measures are providing security to the online transactions and all other online activities.

**Integrity:** Safe the data from altered.

**Confidentiality:** Protect the capturing data packets from hackers.

**Availability:** Keep the data for genuine users.

**Authentication:** Provides permission to access the system based on the identity.

Intrusion in the network that threats the above security measures. This can be done by an inside or outside agent to gain unauthorized entry and control of the security mechanism.

## 2 Intrusion detection system

To protect infrastructure of network systems, Intrusion Detection Systems (IDSs) provide well established mechanisms, which gather and analyze information from various areas within a host or a network to identify possible security breaches.

The Intrusion Detection System (IDS) is introduced that monitors network traffic and suspicious activity and alerts the system or network administrator. In some cases the IDS may take action against them.

We classify the intruders into two types: External and Internal. External Intruders are unauthorized users of the machines they attack, whereas internal intruders have permission to access the system, but do not have privileges for the root or super user mode.

An Internal Intruder may violate the privileges and login as other users with legitimate access to sensitive data whereas a secret.

Intrusion Detection System classified has given below based on function.

### 2.1 Host Based Intrusion Detection System (HIDS)

Anti-threatsoftware's are installed on every network computer.A HIDS might detect internal activity such as which program accesses what resources and attempts illegitimate access. It analyzes the internals of a computing system rather than its external interfaces.

### 2.2 Network Based Intrusion Detection System (NIDS)

Anti-threatsoftware's are installed between the networks. The NIDS reads all incoming packets or flows, trying to find suspicious patterns. NIDS deals with detecting intrusion attacks launched by outside attackers who want to gain unauthorized access to the network to steal information or to disrupt the network.

### 2.3 Signature Based Intrusion Detection System (SIDS)

Searching network traffic for a series of bytes or packet sequencesand compares with predefined specific patterns for attacks.

### 2.4 Anomaly Based Intrusion Detection System (AIDS)

Abnormal behavior or deviation in normal behavior is to be considered as attacks. The system detects can detect known as well as unknown attacks. It tries to identify unusual patterns.

## 3 Proposed system

The Proposed system is composed of the following actions. Collect Network Traffic events, Abnormal Behavioral Activities (Such as repeatedly entered wrong password, etc.), Deviation in Normal BehaviorActivities (such as long time taken to enter user name or password).

The collected data is analyzed using Data Mining

- *[1]K.Mohanapriya M.Sc., M-Phil., M.C.A., B.Ed., Guest Lecturer, Department of Computer Science, Government Arts College for Women, Krishnagiri. E-mail: kmpriya4@yahoo.co.in*
- *[2]Dr.M.Savitha Devi, M.Sc. ,M-Phil., M.C.A., B.Ed., Ph.D., Asst. Professor, Department of Computer Science, Periyar University Constituent College of Arts & Science, Harur, E-mail: savithasanma@gmail.com*

algorithms and Techniques (e.g., classification, clustering, etc.).Detect the intrusion in network and Analyzes intrusion results. Takes decisions on detected intrusions, checks for false positive occurs when an IDS reports as an intrusion an event that is in fact legitimate network activity and a false negative occurs when the IDS fails to detect malicious network activity, controls system operation, generates a performance report and decides if any changes/updates are needed.

## 4 Data mining concepts

A common approach to identifying anomalous objects known as Supervised Learning or Classification is to learn from training datasets, which include Normal or Abnormal instances to make a model. The Abnormal instances then can be identified if they significantly differ from the model. This needs a rich dataset in terms of proper labeling to make an accurate prediction. In the supervised mode, anomaly detection techniques assume that there exists a training data set in which instances have been labeled into normal and anomaly classes. Any unobserved data instance is analyzed by the predictive model, which is built by this approach of deciding whether it is normal or not.

In the Unsupervised Mode, Anomaly Detection Techniques do not need training data. This type of technique which is widely used implicitly assumes that normal instances are more common than anomalies in the data. In these Clustering based methods the false alarm rate will be increased if this assumption is not accurate. Several Semi Supervised Techniques can work in unsupervised mode by employing an unlabeled dataset sample as training datasets if the number of anomalies was very few compared to the whole dataset.

Clustering based techniques are developed by the following concepts. One group assumes that normal data instances fit in a cluster; anomalies do not fit in any cluster, they appear as outliers. The other group assumes that whilst normal data instances sit by their nearest cluster centroid, anomalies are far from their nearest cluster centroid. The third group assumes data instances are normal if they fit in large and dense clusters and anomalies if they fit in small or sparse clusters.

## 5 Network behavior analysis

Network Behavior Analysis is the ability to identify traffic patterns that are not considered normal in the day to day traffic of the network. Simply put this is the industry's attempt to identify irregularities in the network beyond simple threshold settings for excessive traffic. One of the most watched for network security breaches is an abnormal traffic pattern known as a Distributed Denial of Service attack. It is a significant security threat to internet service providers and large network infrastructures.

## 6 Tools

The following tools are used for Intrusion Detection and Prevention System.

### 6.1 Snort

Snort's open source Network Based Intrusion Detection System (NIDS) has the ability to perform real time traffic analysis and packet logging on Internet Protocol (IP) Networks. Snort performs Protocol Analysis, Content Searching and Matching.

### 6.2Suricata

Suricata is an Open Source; fast and highly Robust Network Intrusion Detection System developed by the Open Information Security Foundation. The Suricata Engine is capable of handling real time Intrusion Detection, Intrusion Prevention and Network Security Monitoring. Suricata consists of a few modules like Capturing, Collection, Decoding, Detection and Output. It captures traffic passing in one flow before decoding, which is highly optimal.

### 6.3 Weka

Weka is a collection of Machine Learning Algorithms for Data Mining Tasks. The algorithms can either be applied directly to a dataset or called from your own Java Code. Weka features include Machine Learning, Preprocessing, Classification, Regression, Clustering, Association Rulesand AttributeSelection, Experiments, Work Flow and Visualization.

### 6.4 Anomaly Detection R Package

Anomaly Detection is an Open- Source R Package to detect Anomalies which is Robust, from a statistical standpoint, in the presence of seasonality and an underlying trend. The Anomaly Detection Package can be used in wide variety of contexts.

### 6.5 Rapid Miner

Rapid Miner provides an integrated environment for Machine Learning, Data Mining, Text Mining, Predictive Analytics and Business Analytics and is used for business and industrial applications as well as for Research, Education, Training, Rapid Prototyping, and Application Development. Rapid Miner supports all steps of the Data Mining process including Results, Visualization, Validation and Optimization.

## 7 Conclusion

Recent years, increase in the usage of computers and mobile over Internet for Social Networks, Healthcare, E-commerce, Bank Transactions and many other services. The Networks allow users to create a profile including their Personal Information, to add other users as friends and to exchange messages. It opens the door for unlawful activities. Existing Anomaly Detection Algorithms which are applied to online Networks are limited because of issues such as Complexity, Low Accuracy and Privacy. Using Data Mining concepts for Network Security makes us secure communication in Public Networks.

## REFERENCES

[1] G.K. Gupta "Introduction to data mining with case studies".
[2] Tan .P. N, Steinbach .M & Kumar .V (2005) "Introduction to data mining" Pearson Addison Wesley.
[3] Chakraborty .S, Nagwan .N. K &Dey .L (2011), "Performance Comparison of Incremental K-means and Incremental DBSCAN Algorithms", International Journal of Computer Applications.
[4] Chandola.V, Banerjee.A&Kumar.V (2009) "Anomaly detection: A survey", ACM Computing Surveys (CSUR).

## ACKNOWLEDGEMENT

I am K.Mohanapriya working as Guest Lecturer in Department of Computer Science at Government Arts College For Women, Krishnagiri.
I would like to express my heartfelt thanks and sincere gratitude to my advisor Prof. Dr.M.Savitha Devi, M.Sc., M.Phil., M.C.A., B.Ed., Ph.D., Asst. Professor cum HOD, Department of Computer Science, Periyar University Constituent College of Arts & Science, Harur, who moderated this paper and in that line improved the manuscript significantly. Her immense knowledge and guidance helped me in complete this paper for presentation.
Also My graceful thanks to beloved principal and Head of the Department of Computer Science to give me opportunity to prepare this paper.