IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 9, Issue 6, June 2020

Experimental Analysis of Data Mining Application for Intrusion Detection with Feature Reduction

Jeevitha R[2], Ganagavalli K[2]

Bannari Amman Institute of Technology[1,2]

Abstract: The reliability and availability of network services is under threat as Denial-of-Service (DoS) attacks develop. It needs efficient mechanisms for detecting DoS attacks. Investigate and derive second- order information from traffic data found on the network. Such second-order statistics derived from the proposed approach to analysis may provide valuable correlative information that is concealed among the apps. Through using this secret information, the accuracy of detection can be significantly improved. Comparisons also show that our Cyber Crime based detection approach by Applying Data Mining techniques outperforms some other existing DoS attack detection work.

Keywords: Denial- of-Service (DoS), TCP & UDP, Local to User (R2L), Network Intrusion Detection Systems (NIDS).

I. INTRODUCTION

Data mining is defined as a method by which to obtain usable data from any wider new data set. It involves the analysis of data trends in big quantities of information using one or more applications. Data mining has many applications, such as research and analytics. Data mining calls for effective data collection and storage, as well as computer processing. Uses sophisticated algorithms in information gathering. To classify the data and assess the probability of upcoming events, clustering based on identifying and visually documenting groups of previously unknown information. The actual function of data mining is to search vast amounts of data sort of semi-automatically or automatically to find previously unknown, interesting patterns such as data record classes (cluster analysis), irregular records (anomaly detection), and dependencies. Such patterns can be interpreted as interpretations of input data, and can be used in further study.

A Computer DoS Attack is a cyber-attack that attempts to disconnect a computer or network resource from a host's Internet linked services on a temporary or permanent basis by the attacker's attempt to disconnect its intended users. The received stream of the victim's traffic originates from several outlets during a distributed denial—attack (DDoS attack) Simply blocking a single source effectively prevents an attack. Hackers often attack websites and websites placed on strong-profile operating systems, such as accounts or gateways to loans. These attacks can be triggered by intimidation, violence and activism.

II. METHODOLGY

A. Networking Overview

In the field of network communication, TCP / IP is widely used, consisting of four layers. The application layer transmits and receives router-to- client data via ip address, Google books and Html. TCP and UDP (user datagram log) is used for transport layers to store data. It also gives the error and state details. . The layer or hardware layer linking data includes communication of physical network devices, including wires, antennas, sockets and adapters and other attacks.

B. Network Attacks

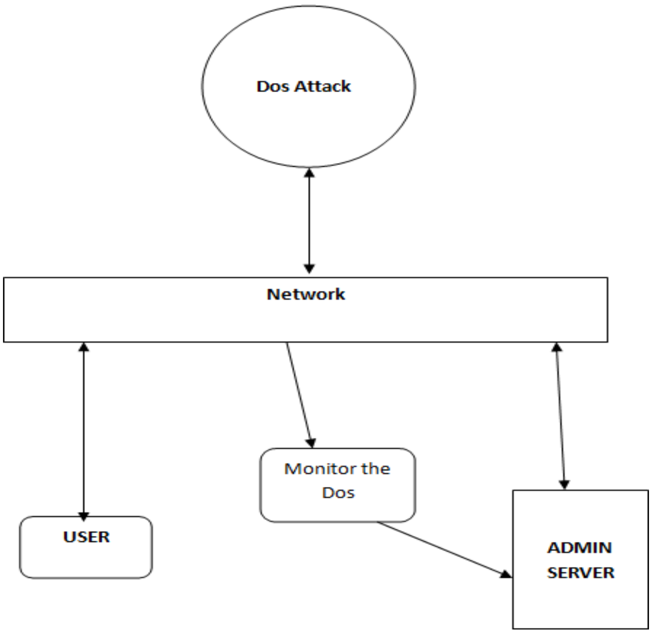
Cyber-crime, which affects Internet companies 'devices, is currently the most dangerous crime committed online. Attacks by computers potentially threaten the protection of a system in many possible state. The form of attack can allow the computer to be provided by a hacker with a control system but it does not. Simulated everyday user activities such as website access create natural connections to the file upload. Owing to a Denial Service (DoS) attack used to block legatine. Users from accessing their Website, a target computer processing power or memory is many occupied. Local to User (R2L) is the assault in the absence of a remote user accessing a local user /device.

C. Intrusion Detection System

It is a software system that monitors a network's activities, such as suspicious behavior, device assault and violence. Anomaly identification and harassment are two primary forms of IDS approaches. Misuse detection relies on signatures for known attacks and anomalies detecting unknown attacks but with a high false positive rate, Misuse detection. This is why the Network Intrusion Detection Systems (NIDS) is becoming a valuable function. Most NIDSs based on anomalies require the use of guided algorithms. The performance of these algorithms depends heavily on the dataset, but in the real-world network context it is hard to obtain such development data. Nevertheless, as channels expand, it's also a concern.

DOI 10.17148/IJARCCE.2020.9625

III. MODULES



A. Login

Normally logging in is used to access a particular page which trespassers can not access. After signing in, you can use the authentication token to track what actions the user took while logging in to the site.

B. User Registration

This module is User registration; all new users must register. Every user is given a unique password with their user name. To access their account, they must provide their correct username and password, i.e. authentication and security is given for their account.

C. Threshold DoS Attack

The threshold is a value. The threshold is correlated with a (Polled Data) statistic. The corresponding threshold value shall be compared when collecting data for that statistics. If the collected data value does not meet the Threshold value then this type of data will result in poor device or network performance. Along with a level, we can set a threshold value such as the maximum value, the minimum value and the equivalent.

IV. ALGORIHMS

A. DDOS Attack Detection Algorithms

Distributed Denial of Service (DDoS) Attack is a serious threat to the Internet. It's hard to identify the signature of the same Attack. Moreover, it is difficult to discern the difference between an excessive amount of traffic that is triggered by an attack or occurs when a large number of users visit the target system on a regular basis at the same time. Entropy detection is an effective technique for identifying a DDoS attack. This is primarily used to measure the randomness of the distribution of these attributes in the network packet headers. In this article, we are focusing on DDoS attack detection technology. Develop the recent entropy tracking algorithm and provide two improved methods based on combined gravitation and moment, respectively. The results of the experiments indicate that such techniques can detect DDoS more precisely.

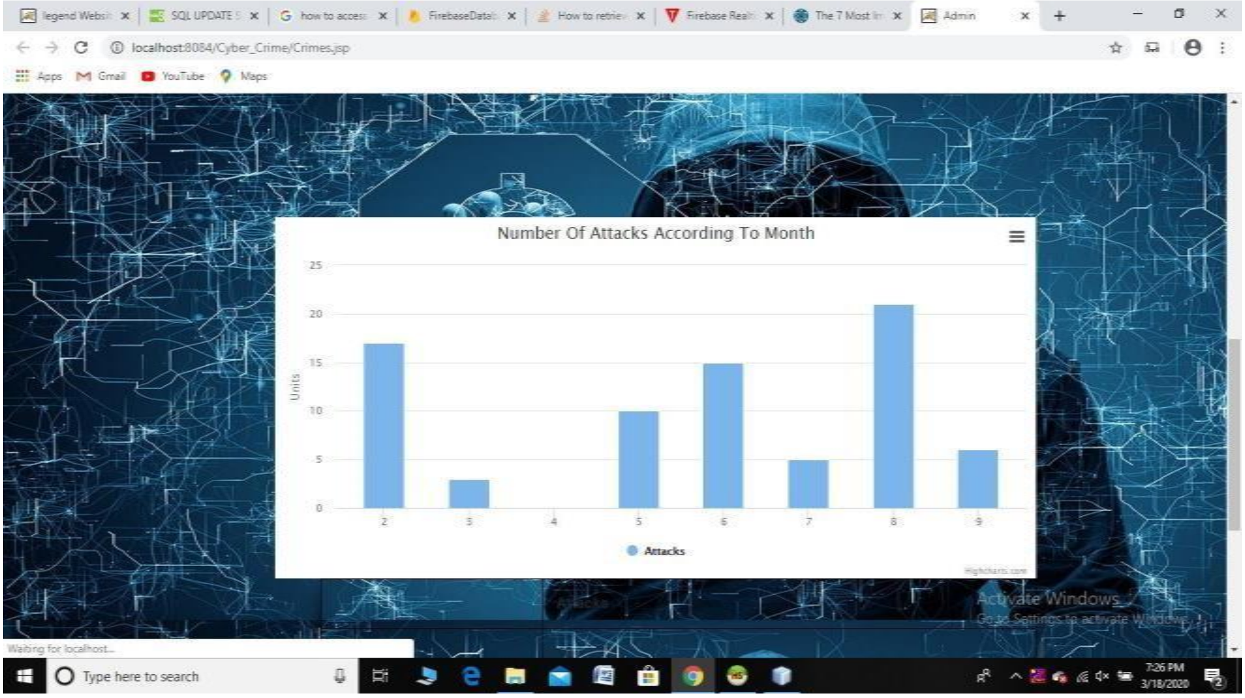
B. Association

Association is analogous to an analysis of patterns, but it is popular in dependent samples. In this case, you will look for specific events or attributes that are closely correlated with another event or attribute; you will find, for example, that when your customers purchase a particular item, they will frequently purchase a similar item for one second. It is usually what's used to fill "people ordered" online retailers sites.

C. Clustering

Clustering is somewhat similar to sorting, except it requires grouping together pieces of data dependent on connections. For instance, you might choose to package the different demographics of your audience into different packages based on how much disposable income they have, or how much theywant to shop in your store.

DOI 10.17148/IJARCCE.2020.9625



V. CONCLUSION

The DoS attacks have been detected using data mining techniques. In IT field this is endanger and mostly risky. The server gives the limited notification and sending regular requests. The network traffic packets are high to increase the storage capacity. The introduction to the cybercrime using various data mining techniques. The pattern recognition is the common technique used here. The limit should be set. The admin will be notified when the server receives the number of similar requests is more than the value of the set for threshold, It will be an attack. Using this method it can easily been recognize DoS attack or hacker is sending many request to reduce the efficacy of the server in DoS attack.

The strong believe that the safest and most effective way to counter DoS attacks might be a completely secure real time defense framework. The hope to see sooner in the near future, by creating a security framework as close to the source of the attack with the avoidable interference of various service providers providing a source address validation and filtering functionality.

REFERENCES

[1] M.Khan , S.K.Pradhan, M.A.Khaleel, “Outlier Detection for Business Intelligence using data mining techniques”, International journal of Computer Applications (0975 -8887), Volume 106-No. 2, November 2014.
[2] Masud, M.M, Gao,J.Khan, ”Peer to Peer Botnet Detection for Cyber Security: A Data Mining Approach”. In proceedings: Cyber-security and information Intelligence research workshop.Oakridge national Laboratory, Oakridge May 2008.
[3] Internet Security Threat Report, Volume 21, April 2016, Symantec Crime Report.
[4] Ibrahim Salim, T.A.Razzack,”A study on IDS for Preventing denial of service attack using outliers techniques”, 2nd IEEE international conference on Engineering and technology, March 20