International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 01 | Jan 2019 www.irjet.net p-ISSN: 2395-0072

INTRUSION DETECTION SYSTEM USING CLOUD COMPUTING

Aayushi Kaur Kochar[1], Deepali Jawale[2], Sayali Khomane[3], Sharvari Kamble[4]

[1,2,3,4] *BE (Computer Engineering), Modern Education Society's College of Engineering*
Professor.A.P.Kale, Dept. of Computer Engineering, Modern Education Society's College of Engineering, Maharashtra, India

---

Abstract - *Many systems use servers to manage and store their data, sometimes the servers are slowed down because of multiple user requests. Most of which are attackers or unauthorized users and some are genuine users. In computing, a denial-of-service (DoS) attack is an attempt to make a machine or network resource unavailable to its intended users. A Distributed Denial of Service (DDoS) attack is an attempt to make an online service unavailable by overwhelming it with traffic from multiple sources. They target a wide variety of important resources, from banks to news websites, and present a major challenge to making sure people can publish and access important information.*

A distributed denial-of service (DDoS) is where the attack source is more than one, often thousands of unique IP addresses. Flooding is one of the typical DDoS attacks that exploit normal TCP connections between a client and a target web server. In this project we are trying to devise a DDoS anomaly detection method on Cloud that implements a detection algorithm against the Flooding attacks.

Key Words: DDoS, unauthorized users, Intrusion Detection System

1. INTRODUCTION

When multiple users are trying to make a request on the server for a particular service, there might be some users who will be bad users. These bad users try to either slow down the server or do some malicious activities that might be inappropriate. Also these bad users might try to hang the system. This is where the Distributed-Denial-Of-Service(DDoS) attacks come into picture. DDoS attacks are the attacks where multiple attackers are trying to attack on the server or slow down the server. There are many such examples of DDoS attacks. Social websites such as Amazon and Flipkart can be examples where the DDoS attacks take place. There are multiple clients who are trying to make a request and buy products in these websites. Due to this there can be a possibility of either slowing down the system or hanging up the website. Thus, DDoS attack needs to be completely prevented.

A common type of DDoS attack is IP spoof attack. An example of this type of attack is SYN Floods attacks. In computer networking, the communication takes place through exchange of network packets. These network packets consist of multiple headers. The two types of headers used are Source IP address and Destination IP address. The Source IP address is the address of the sender during the exchange of packets. IP address spoofing is the type of attack in which it falsifies the content in the header of the Source IP address either to mask the sender's identity or to cause DDoS attacks to take place. Thus, IP spoofing attacks are the attacks in which the attacker uses a false IP address other than the original IP address. Thus, preventive measures need to be taken to avoid such attacks.

2. MOTIVATION

An intrusion detection system (IDS) is a system that monitors network traffic for suspicious activity and issues alerts when such activity is discovered. DDoS attacks may result in system performance degradation of the targeted network. The services intended to the genuine users may not function or may produce delayed results. Distributed Denial of Service (DDoS) flooding attacks are one of the biggest concerns for the security and network professionals.

Many commercial institutes make use of Cloud for data and transaction handling. DDoS attack can lead to degradation or can also hamper the overall system performance. The goal of intrusion detection is to build a system is to keep a track of the activities of the network and to detect such DDoS attacks. Once an attack is detected, the system administrator could be informed and thus take corrective action. Thus, the motivation of the project is to develop security in the systems by avoiding the DDoS attacks. Also, quick detection of intrusions can help to identify intruders and limit damage.

2. 1 INTRUSION DETECTION SYSTEMS:

In the recent years, there has been a rapid increase in the usage of Internet which has caused more number of attackers to do malicious activities. An Intrusion Detection System (IDS) is a device or software application that monitors a network or systems for malicious activity or policy violations. Many organizations often make use of firewall to protect their networks from malicious activities. A more advancement on firewalls can be done by making use of Intrusion Detection Systems. Thus IDS is treated as a second line of defense for protecting private networks against malicious activities. Intrusion detection is important for business organization, system applications and for large number of servers and on-line services running in the

system. Hence enhancing the efficiency of IDS is equally important.

Intrusion Detection System compromises a computer by breaking its security and thereby letting the computer enter into an insecure state. If such an event takes place, the computer becomes vulnerable to several attacks. These attacks aim to obtain information about the target computer and this information obtained can be used to conduct fraudulent activities. It is difficult to prevent an intrusion from entering the system but if these computer intrusions are detected in time, the administrator can be informed and necessary actions can be taken at early stages. For this purpose, we use an Intrusion detection system (IDS). In this project we are trying to devise a DDoS anomaly detection method on Cloud that implements a detection algorithm against the Flooding attacks.

2. 2 TYPES OF IDS:

1) HOST BASED INTRUSION DETECTION SYSTEM :

Host based intrusion detection system (HIDS) monitors the activities of an individual host or computer system. The primary focus is on the operating system activities and events. However, in network systems also, HIDS finds its best values in finding the flow of information and detecting the attacks over the network based on the events occurred within the network.

2) NETWORK BASED INTRUSION DETECTION SYSTEM :

A network based intrusion detection system can at any single instance of time monitors multiple systems in a network in parallel. NIDS finds its best values when each single packet is analyzed that is about to move into the network through the firewall implemented above the network and thus helps in monitoring the information traversing through the network and detects any intrusion activities.

3. LITERATURE SURVEY:

Hyo-Sang Shin, Dario Turchi, Shaoming He, and Antonios Tsourdos have made use of pattern matching techniques for behaviour anomaly detection. Network behaviour anomaly detection is one technique for providing security throughout the network. It continuously monitors and tracks the network to determine malicous activities or unusual trends. In this paper the behaviour anomaly detection is performed in a scenario such as moving vehicles. Besides moving vehicles this technique can also be applied on trains, airports, road incidents, etc. This paper consists of two important components namely trajectory analysis tool and a string matching method. The string matching method used in this paper is based on Regular Expressions. [1]

Vandana B. Salve, Vishwayogita Savalkar and Sonali Mhatre have made use of four pattern matching algorithms namely KMP algorithm, BM algorithm, Enhanced BM algorithm and One Enhanced BM algorithm. Intrusion Detection System(IDS) is widely used to detect malicious activities done by multiple users on the system. There are various methods and algorithms that can be used for carrying out the Intrusion Detection System. One such method is by using pattern matching. In this a pattern is created and the user's activity is compared. If the resultant pattern does not match with the usual pattern, then intrusion can be detected.[2]

Bahman Rashidi, Carol Fung, and Elisa Bertino have proposed a DDos defence mechanism named as CoFence. This defence mechanism facilitates a domain-helps-domain collaboration network among NFV-based domain networks. Network functions Virtualization(NFV) offers a method to design networking services. NFV makes use of different network functions such as network addresses so that they can run in software. The Distributed Denial Of Service(DDoS) attacks are tremendously increasing day by day. A common type of these attacks called as SYN flood attacks is of major damage and should be completely avoided. Thus in this paper the authors have focused more on SYN flood attacks to detect and prevent them. By making use of CoFence, they have introduced resource sharing among networks so that they can handle these large volumes of DDoS attacks. They have typically used dynamic resource allocation so that the resource allocation is efficient and compatible.[3]

Akash Garg and Prachi Maheshwari reviewed snort as misuse based intrusion detection system as well as ALAD, PHAD, LERAD, NETAD. Network security has become very essential in today's time. Maintaining network security has become very difficult as more and more computer networks are being used. Snort is a method which is typically used to maintain this network security and is a network intrusion prevention system. It is used to keep a track of the network and prevent any unauthorized access or malicious activities thus providing network security. Usually firewalls are used to provide security but they are not much efficient because they only detect attacks taking place which are coming from outside the network. Thus, more preventive measures must be taken. Hence, in this paper authors have focused more on Snort as a method to provide network security. [4]

Yonghong Chen, Xin Chen, Hui Tian, Tian Wang, Yiqiao Cai have proposed a method to deal with IP spoofing. Since in IP spoofing attacks, the attackers makes use of fake Source IP addresses, thus the authors have made an attempt to identify the real source of the DDoS attack packets. They have made use of clustering methods so that they can identify the real source of number of packets. Identifying the real source of a single packet is difficult and time consuming. Thus they have made use of clustering methods to identify a cluster of real sources of the packets. The authors have made use of K-harmonic means clustering method. This method determines

the best number of clusters so that tracing the real source can be much easier. [5]

Naveen Mohan Prajapatil, Atish Mishra and Praveen Bhanodia have presented an overview of existing intrusion detection techniques for DDoS attacks. They have considered different intrusion detection techniques that are used today and have compared their performance based on both their run time performance and the considerations made theoretically. After comparing and analyzing the results, they have found out the most useful and important intrusion detection system technique. They have also given a detailed scenario of each technique and have mentioned what their strengths and weaknesses are. They have introduced what Intrusion Detection System is and have explained the characteristics of IDS. After viewing the results the authors have concluded that the performance of the algorithms and techniques used so far are more or less the same as they were expected. [6]

Vibha Gupta, Maninder Singh and Vinod K. Bhalla used four pattern matching algorithms namely Brute-force, RabinKarp, Boyer Moore and Knuth-Morris-Pratt for the analysis. In this paper, focus has been made on the signatures of known attacks. Intrusion Detection and Prevention Systems (IDPSs) are used for the purpose of detecting intrusion in the system. These systems use signature of the attacks to detect them. These signatures are identified by various pattern matching algorithms. Thus, by using these four pattern matching algorithms signatures of the known attacks are identified to prevent them.[7]

Akashdeep Bhardwaj, Dr. Vinay Avasthi and Dr. Hanumat G Sastry have proposed solutions for DDoS attacks on Cloud. In today's day to day life Internet is growing tremendously and is used by many organizations and institutes. The cyber terrorists and hackers know this fact too and can attack the network on a large scale. These attackers make use of Distributed Denial Of Service attack to attack the Internet. Using these attacks they can either slow down the website or hang the system. Due to the rapid increase of Internet, more and more attackers are trying to destroy the Internet and slow down the system using DDoS attacks. Thus, in this paper the authors have proposed various solutions to deal with this serious problem and to avoid attackers to destroy the system by detecting and preventing DDoS attacks. These attacks mainly deny access to the users to using the Internet. Denial Of Service attacks are a type of cybercrime attacks that deny the users of the system the access to various online web applications, social websites, etc. on a large scale. Thus an attempt to provide solutions to these attacks is done in this paper.[8]

Zeeshan Ahmed Khan, R.K Pateriya have proposed the comparison between different multiple pattern string matching algorithms. A comparison of algorithms like Aho-Corasick, BitParallel (Shift-OR), Rabin-Karp, etc. type of string matching algorithms is presented in this paper. The authors have focused on the usage of string matching algorithms for the purpose of assuring data security. Thus in this paper the authors have used various string matching algorithms and have compared their results and their performance based on various parameters.[9]

Disha Sharma has focused on the usage of clustering to be used for intrusion detection. Clustering can widely be used for the purpose of Intrusion Detection System and is very beneficial. As the attacks are changing day by day and as the usage of Internet is increasing, there is need to define more developed methods to be used for IDS. The author has used the Fuzzy c-medoids algorithm as a clustering technique that can be used for intrusion detection. In this paper, the focus is made on fuzzy algorithms and has also given a comparison of fuzzy k-medoid and fizzy c-medoid algorithms. From the comparison, the author has concluded that which fuzzy clustering algorithm can be used best for the purpose of Intrusion Detection.[10]

4. PROJECT SCOPE:

In computing, a denial-of-service (DoS) attack is an attempt to make a machine or network resource unavailable to its intended users, such as to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet. A distributed denial-of-service (DDoS) is where the attack source is more than one, often thousands of, unique IP addresses.

We will build an Intrusion Detection System that will determine the DDoS attacks. We will be using detection based algorithm to determine malicious activities for intrusion detection that will be able to distinguish between an attack and non-attack so as to increase detection accuracy and reduce false alarm rate. The scope of the project is to provide the security in Server, we are proposing a new methodology known as IDS on Cloud. It prevents the unauthorized access and hacking of data. The project can be used by organizations that include Cloud and are facing various such malicious activities by attackers.

5. CONCLUSIONS

The DDoS attacks are high risk factors, particularly flooding attack, which is one of the easiest to implement but one of the most effective type of attack as well. The Report reviews the implementation of an efficient program which will not only detect the live DDoS attack on Cloud, but also avoid it, thus ensuring the smooth functioning of the system, as well as optimal performance without performance overhead. The project can be implemented by companies with cloud based data store in order to avoid flooding or DDoS attack thus keeping it to maximum efficiency.

Distributed Denial of Service (DDoS) Flooding attacks are one of the biggest concerns for the security and network professionals. Most of the leading commercial institutes make use of Cloud for data and transaction handling. DDoS attack destroys the network security which can degrade or hamper the overall performance. This work presents a program which will not only detect the live DDoS attack on cloud, but also avoid it.

REFERENCES

[1] Vandana B. Salve, Vishwayogita Savalkar, Sonali Mhatre,"Efficient Pattern Matching Algorithms in IDS" in Proceedings of the Second International Conference on Inventive Systems and Control (ICISC 2018).

[2] Hyo-Sang Shin, Dario Turchi, Shaoming He, and Antonios Tsourdos, "Behavior Monitoring Using Learning Techniques and Regular-Expressions-Based Pattern Matching", in IEEE transactions on intelligent transportation systems,2018.

[3] Bahman Rashidi, Carol Fung, and Elisa Bertino, "A Collaborative DDoS Defence Framework using Network Function Virtualization", in IEEE Transactions on Information Forensics and Security 1,2016.

[4] Akash Garg and Prachi Maheshwari,"A Hybrid Intrusion Detection System: A Review", in IEEE Transactions on Information Forensics and Security 1, 2016.

[5] Yonghong Chen, Xin Chen, Hui Tian, Tian Wang, Yiqiao Cai, "A Blind Detection Method for Tracing the Real Source of DDoS Attack Packets by Cluster Matching", 2016 8th IEEE International Conference on Communication Software and Networks.

[6] Naveen Mohan Prajapatil, Atish Mishra and Praveen Bhanodia,"Literature Survey - IDS for DDoS Attacks", in IEEE Transactions on Information Forensics and Security 1, 2014.

[7] Vibha Gupta, Maninder Singh and Vinod K. Bhalla,
" Pattern Matching Algorithms for Intrusion Detection and Prevention System: A Comparative Analysis", in IEEE Transactions on Information Forensics and Security 1, 2014.

[8] Akashdeep Bhardwaj, Dr. Vinay Avasthi and Dr. Hanumat G Sastry, "Solutions for DDoS Attacks on Cloud", in IEEE Transactions on Information Forensics and Security 1,2016.

[9] Zeeshan Ahmed Khan and R.K Pateriya, "Multiple Pattern String Matching Methodologies: A Comparative Analysis", in International Journal of Scientific and Research Publications, Volume 2, Issue 7, July 2012.

[10] Disha Sharma, "Fuzzy Clustering as an Intrusion Detection Technique", in International Journal of Computer Science & Communication Networks, Vol 1(1), September-October 2011.