An Overview of DDoS Attack Detection in Cloud Computing

Shaikh Md Muzammil
U.G Student
Department of Information Technology
B. K. Birla College of Arts, Commerce, & Science (Autonomous), Kalyan, Maharashtra, India

Abstract— Cloud computing is an emerging technology in today's raising scenario. One of the major threats to Cloud security is Distributed Denial of Service Attack (DDoS) or simply Denial of service attack (DoS) in the virtual machines. Here, the DoS attack is overcome using hop-count filtering methodology and sequence number encoding strategy and DDoS is a combination of DOS attack where multiple compromised systems, are infected with a Trojan and their target is a single system and their result is inflicting a Denial of Service (DoS) attack. In this paper, a complete survey and analysis of various Distributed Denial of Service Attack detection and prevention technique is studied and discussed so that on the basis of problems surfaced, a new, renewed and efficient technique is implemented for the detection and prevention of Distributed Denial of Service Attack especially in Cloud Computing System.

Keywords: Cloud computing, Denial of Service, Distributed Denial of Service, Security, Detection, Prevention

I. INTRODUCTION

Cloud Computing is an evolving model that is growing rapidly and is a modern model that is intended to provide suitable, on-demand, network access to a common group of configurable computing resources "as a service" on the Internet for satisfying computing demands of the users. Services on the Cloud are sent by the Internet. Due to this security and privacy of Cloud resources, data and existing services are the main concerns in cloud. So many security problems come when we use cloud computing - First is the Security problem faced by cloud computing providers and the second is the issue faced by the cloud computing customers. In most of the cases, the provider must make sure that their framework is protected and that their customers' data and applications are protected. On the other hand, customer also wants to guarantee that the provider has exerted proper security actions to protect their information.

So many traditional attacks affect the working of cloud computing, these attacks affect the integrity, confidentiality, and the availability of Cloud properties and current services and are present at the network layer. These attacks are DNS Poisoning, Denial of Service (DoS), Address Resolution Protocol (ARP) spoofing, Distributed Denial of Service (DDoS), IP Spoofing, man-in-the middle attack, port scanning, Insider attack, Routing Information Protocol (RIP) etc.

Firewall is the border access points of system and it provides safety at first place i.e., at the border of any atmosphere or network. Since firewall detects the network packages only at the boundary of any network, then insider attacks cannot be found using this. Some attacks which belong to DoS or DDoS are too hard to detect by using usual firewall. As a result of that, usage of firewalls to block all the intrusions is not an effective solution. Another technique we can employ is to combine Cloud computing with network-based detection system (NIDS). NIDS do the function to au-courant system and it adds protective layer which provide security by detecting attacks which induces our system. Two techniques can be used in NIDS. One is the signature-based detection method that can be used to detect known attacks professionally. The other method can be anomaly detection method that finds the behavior of packet or user is malicious or not. NIDS efficiency depends on the parameters used in the detection method, its position in the network means where NIDS is located i.e., in front or at back end, how system organizes or configures centralized or distributed environment.

A. Types of Cloud Computing

1) Delivery Model

Delivery model is of four types in Cloud Computing, they are:

2) Public Cloud

In Public cloud computing, the cloud provider makes the resources available to the customers over the Internet which is public network. Usually the documents of the corporation which uses the public cloud are kept external to its location by a third party whom they trust. This increases the risk of information privacy and security because of cloud structure in which computers, network and storage is placed outside the company's firewall.

B. Private Cloud

In the private cloud, the association allows own resources over its private network. The company owns the services, resources and defines which users can access it. The security risks are also reduced because all things are accomplished inside the enterprise or association. Firewall allows a fair use of the applications and the network bandwidth.

C. Hybrid cloud

Hybrid cloud is a computing platform, which combines, or we can say make connection between private cloud and public cloud. It is installed by organizations, which do not want to put all things in the external cloud (i.e., public cloud) while hosting some servers in their own internal cloud structure. The provider of the Cloud can process applications which can work in between those limitations.

D. Community cloud

A community cloud is a platform, which allows corporations to share resources and infrastructure over a common cloud environment. The condition for this is that they should belong to same industry and they do the similar type of operations. It is organized and provided by one company and used by the others or provided by a third party over the Internet.

E. Service Model

1) Software as a Service (SaaS)

This is the most important model from user's point of view. In this model, cloud provider installs and functions different application software's in the cloud environment. The cloud users can access these software's from cloud customers but do not directly access the infrastructure of Cloud as well as platform on which the particular application is running i.e. , the users can access the software online and can store the data back in the cloud. It removes the need of installing the application on the user's own computers system. This feature provides basic maintenance and support for different levels of user accountability.

2) Platform as a Service (PaaS)

It is another application delivery model which offers platform, or we can say: all the required resources to run any application without installing or downloading it. This package includes design, development, hosting, testing and deployment for any application or software. PaaS also delivers support for the creation of user interface which is based on HTML or JavaScript.

3) Infrastructure as a Service (IaaS)

It is an application in which limited number of properties is easily allocated to large number of users. Infrastructure refers to the operating system and its virtualization that is how efficiently it accomplishes resources without administering background details. Dedicated CPU is allocated; moreover, they access the virtual memory conferring to their accountability in cloud environment.

SaaS and PaaS are used to offer application services to the user, whereas IaaS is used to offer hardware services so that organization can lay whatever they want to nail onto it.

4) Distributed Denial of Service Attack

Distributed denial of service (DDoS) TCP overflow attacks are DoS attacks in which attackers overflow a victim machine with packets in order to exhaust its resources or consume bandwidth. As the attack may be distributed over multiple machines, it will be very tough to differentiate authentic users from attackers. In fact, a DDoS flood attack is not only a widespread attack; it is the second most common cybercrime attack to cause financial losses according to the United States Federal Bureau of Investigation (FBI).

DDoS attacks can be established in two different ways: either directly and/or indirectly. Direct attacks target a weakness in the system of the target machines and damage the machines directly. On the other hand, indirect attacks do not target victim machines directly; they quarry on other elements with which the victim machines are associated and hinder their work. In the following discussion, the TCP flood attack is used; this is an indirect attack, as it consumes most of the network's resources, meaning that they are not readily accessible to other users. A TCP flood attack was carried out with software on a virtual cloud network; Wireshark Network Analyzer 2.0.0 was used to capture and analyse traffic both before and during the attack.

Firstly, using TCP Ping, we sent 50 TCP test probes to a server (server machine 10.25.129.5:811). The reply took 1.3 ms on average, as shown below: Ping statistics for 10.25.129.5:80 50 probes sent. Approximate trip times in milliseconds: Minimum = 0.25 ms,
Maximum = 26.065 ms,
Average = 1.323 ms

The TCP protocol uses several flags to achieve the state of a connection in the packet header. We focused on two of these, which are used in establishing TCP connections:

- SYN (Synchronize) which indicates the initiation of a connection; and
- ACK (Acknowledge) which indicates data received. We monitored the traffic of the 50 probes at the server machine using Wireshark, by capturing the packages that were connected with the server using the filter ''ip.addr = = 10.25.129.5''. As the traffic was normal, the server machine responded to all requested packets according to the TCP protocol.

F. During the attack

An attack was launched using a software program which performed a DDoS TCP flood attack on a specific server. Once the DDoS TCP flood attack underway on the victim machine in the cloud, the arriving packets were much more numerous than the server could handle. Consequently, the server could not respond to all the requesting packets from whichever normal users or the attackers. Note that 10.25.129.5 was the IP address of the target server and 10.31.133.236 was the IP address of the attacker. The first request packet from the attacker was successful, as it was preserved like a normal requesting packet. The following ones were not successful, as the server was too busy and could not respond. Finally, we sent 50 TCP test probes within a few seconds to the target machine during the attack period to test the connection. The reply time was 9.6 ms on average, which differs significantly from the first test as shown below:

Ping statistics for 10.25.129.5:81 50 pings sent. Estimated times in milliseconds: Minimum = 0.181 ms, Maximum = 152.341 ms, Average = 9.56 ms To sum up, the DDoS TCP flood attack can disturb the cloud server's performance within a short time, slowing down the response, and can even stop the service completely. TCP errors will also be increased. Therefore, an efficient and effective detection and prevention technique is required.

II. Related Work

In [1] Khaleel A. Fakeeh had Given lots of information about DDOS attacks and prevention. They also given numbers of references for the research. This paper proposed that they conducted the survey on DDOS (Distributed Denial of Service) attacks research work and analyzed prevention and detection methods used for DDOS attacks in the cloud. We found that there is a good amount of research scope in detecting and preventing slow client application layer attacks in the cloud.

In [2] Usman Amir stated that As cloud computing is gaining raise day by day and simultaneously the probability of data breaching is also there. They have mentioned 22 types of prevention techniques. It is a hybrid solution for detection and prevention mechanism in which the Honeypot and Firewall works under a single window operation. Honeypot is effectively used for the detection and prevention on the basis of pattern matching and the signatures that already existed can be blocked by firewall. This paper proposed that

they described the use of honeypot. And described types of prevention and also give introduction about intrusion detection system (IDS).

In [3] Pedro Manso stated that The current paper addresses relevant network security vulnerabilities introduced by network devices within the emerging paradigm of Internet of Things (IoT) as well as the urgent need to mitigate the negative effects of some types of Distributed Denial of Service (DDoS) attacks that try to explore those security weaknesses. This proposal detects DDoS-based cyber-attack scenarios and limits them at their origin at the client side, this way mitigating the negative consequences of the widespread effect of that attack for potential victims.

[4] This paper presents a novel big-data-framework based NIDS for DDoS attack detection in VANET. The proposed NIDS consists of two main components: the collection module and detection module. Distributed traffic collection technology is adopted and deployed on some important network nodes to collect traffic efficiently. The ML classification algorithm is accepted to categorize the traffic to achieve high accuracy and low FAR. This paper only evaluated the proposed system on public datasets. In future work, they plan to deploy the real environment of the proposed NIDS, and use DDoS tools to launch attacks, and then evaluate the performance of the system.

[5] This paper proposed novel IDS integrating multi-objective-based feature selection and the deep learning methodology for the classification of the DDoS attack. The paper proposed method has achieved a very impressive high accuracy of 99.03% along with an Fl-score value of 99.36 %. They compared the presented method with state-of-the-art techniques, which conclude that our method outperforms other work, which confirms the efficiency of the proposed method.

[6] The paper proposed to study the problem of deploying honeypot for DDoS attacks in SDN. The proposed honeypot strategies in SDN can provide dynamic protection for SDN, and further protect the security of the IIoT devices. Hence, malicious attacks under our strategies can be effectively controlled. The paper proposed a pseudo-honeypot game strategy to analyse the strategic interaction between attackers and defenders. The experiment results have showed that the energy consumption and the defence efficiency can be improved with the proposed strategies.

[7] The paper proposed a total overview and examination of different Distributed Denial of Service Attack recognition and avoidance procedure is dissected and talked about so that based on issues surfaced, another, changed and effective method is actualized for the discovery and anticipation of Distributed Denial of Service Attack particularly in Cloud computing System. The paper proposed that various detection and prevention techniques implemented for the DDoS Attack are analysed and discussed and hence, by analysing the various issues detected in the existing methodologies, it also states that an efficient framework can be implemented for the improvement of low false alarm rate as well as providing better true positive rate for the detection and prevention of DDoS attacks in the cloud computing system.

[8] This paper proposed that CS_DDoS system proposals a solution to securing stored records by classifying the incoming packets and making a decision based on the classification results. Throughout the detection phase, the CS_DDOS identifies and determines whether a packet is normal or originates from an attacker. During the prevention phase, the packets, which are classified as malicious, will be denied accessing the cloud service and the source IP will be blacklisted. The proposed approach can efficiently develop or improve the security of records, reduce bandwidth consumption and mitigate the exhaustion of resources. In the future, we aim to extend CS_DDoS to overcome the problem of DDoS using spoofed IP addresses as well as to improve the work to identify the attackers even when they satisfy the threshold value.

[9] The paper proposed that, to investigate the vulnerability of the cloud platform due to which DDoS attacks happen and the methodology that they use to influence the administration's accessibility. Why the existing defence mechanisms are not sufficient? Also, the impact of DDoS in cloud environment will be discussed in this paper. This paper plays out an examination on current cloud security challenges for example, sharing specialized defects, uncertain interface of Programming interface, malevolent insiders, web convention vulnerabilities and an exhaustive review of already existing defense mechanisms of DDoS in cloud computing.

[10] The paper proposed that they design an efficient security framework which is Protocol specific Multi-threaded Network Intrusion System (PM-NIDS) aiming at detecting DoS/DDoS attacks in the cloud. The paper proposed, it captures the packet, pre-processes it, extracts the network features and passes them to the classifiers for intrusion detection. It uses both signatures based and anomaly-based detection which are complementing each other. Therefore, it can detect known as well as unknown attacks in cloud.

III. Conclusions

In this paper, we discussed different research work conducted on DDOS attacks in Cloud. We listed all information about DDOS attacks, and the methods used to detect and prevent the same in the cloud. We found that however there is a lot of research has been conducted in DDOS attacks for the cloud. As there is several types of DDoS and it is very much difficult to develop the mechanism for all. Therefore, in future work we will concentrate to offer an integrated solution which will be able to deal with any type of DDoS attack and to save our resources from the attackers.

References

[1] Khalid A. Fakeeh "An overview of DDOS attack detection and prevention in the cloud" International Journal of Applied Information Systems (IJAIS) Foundation of Computer Science FCS, New York, USA Volume 11 – No. 7, December 2016.
[2] Usman Amir and Khalid Hussain "DDoS Attacks Detection and Prevention Techniques in Cloud Computing: A Systematic Review" International Journal of Computer Science and Information Security (IJCSIS), Vol. 14, No. 10, October 2016.
[3] Pedro Manso , José Moura , and Carlos Serrão "SDN-Based Intrusion Detection System for Early Detection

and Mitigation of DDoS Attacks" Published: 8 March 2019.

[4] YING GAO , HONGRUI WU , BINJIE SONG, YAQIA JIN, XIONGWEN LUO, AND XING ZENG "A Distributed Network Intrusion Detection System for Distributed Denial of Service Attacks in Vehicular Ad Hoc Network" Department of Computer Science and Engineering, South China University of Technology, Guangzhou 510006, China, October 18, 2019.

[5] Monika Roopak, Prof. Gui Yun Tian, and Prof. Jonathon Chambers "An Intrusion Detection System Against DDoS Attacks in lOT Networks" School of Engineering Newcastle University UK, 2019.

[6] Miao Du, and Kun Wang "An SDN-Enabled Pseudo-Honeypot Strategy for Distributed Denial of Service Attacks in Industrial Internet of Things" IEEE,2019.

[7] DALIMA PARWANI, AMIT DUTTA, PIYUSH KUMAR SHUKLA And MEENU TAHILIYANI "Various Techniques of DDoS Attacks Detection and Prevention at Cloud: A Survey" Oriental Scientific Publishing Co., India, August 2015.

[8] AQEEL SAHIL, DAVID LAI, YAN LI, (Member, IEEE), AND MOHAMMED DIYKH "An Efficient DDoS TCP Flood Attack Detection and Prevention System in a Cloud Environment" IEEE, April 6 2017.

[9] Anupama Mishra, Neena Gupta "Analysis of Cloud Computing Vulnerability against DDoS" Published by IEEE, 2019.

[10] Rajendra Patil, Harsha Dudeja, Snehal, Gawade and Chirag Modi "Protocol specific Multi-threaded Network Intrusion System(PM-NIDS) for DOS/DDOS attack detection in cloud" Published by IEEE, 2018.

[11] Iman Sharafaldin, Arash Habibi Lashkari, Saqib Hakak and Ali A. Ghorban "Developing Realistic Distributed Denial of Service (DDoS) Attack Dataset and Taxonomy" IEEE, 2019.

