Indian Journal of Science and Technology, *Vol 9(38), DOI: 10.17485/ijst/2016/v9i38/98811, October 2016*
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Mitigating Distributed Denial of Service Attack in Cloud Computing Environment using Threshold based Technique

Nitesh Bharot[1*], Veenadhari Suraparaju[1], Sanjeev Gupta[3] and Priyanka Verma[2]

[1]Department of Computer Science and Engineering, Aisect University, Bhopal - 464993, Madhya Pradesh, India; niteshbharot20@gmail.com, veenadhari1@gmail.com
[2]Department of Information Technology, ABV-IIITM, Gwalior - 474015, Madhya Pradesh, India; 303priyanka.verma@gmail.com
[3]Department of Electronics and Communication, Aisect University, Bhopal - 464993, Madhya Pradesh, India; sanjeevgupta73@yahoo.com

Abstract

Objectives: Cloud is becoming a very assertive computing platform now a days due to the availability of resources in a customized manner. But DDoS attack is a very dangerous as it directly affects the availability of resources. So the objective of the paper is to mitigate DDoS attack in cloud network using threshold based technique. **Methods/Statistical Analysis:** In the proposed solution a list of faulty IP addresses has been prepared based on their performance during the Turing test and named as black list. If the request is from black list than it is directly rejected else forwarded to next step. At the second stage check whether the number of resources available are greater than the request made and also the request for resources is less than the threshold value of resource m, than the resource are allocated to that request else request is rejected. **Findings:** Cloud resources can be defended from the DDoS attack by any of the three defense mechanisms, i.e. DDoS attack prevention, DDoS attack detection and DDoS attack mitigation and recovery. But it is found that Attack mitigation is the easiest way to defend against the DDos attack because of easily available resources. The paper presented a technique that will easily detect and mitigate the DDos attack and it is very easy to implement with minimum cost and overhead. **Application/Improvements:** The proposed work can be implemented in any cloud network to save it from wasting the resources for malicious requests. For further improvement client based protection can also be implemented such that the attacker will not be able to form its army for the purpose of DDoS attack.

Keywords: Attack Mitigation, Attack Detection, Cloud Computing, DDoS Attack

1. Introduction

To access the resources, services and application over the internet cloud computing have become a most commodious way. Cloud computing is also known as utility as computing. Cloud computing has the embryonic to commute a huge section of IT industry. In the latest IT trends, Cloud Computing is emerging as a key computing platform for companioning resources like infrastructure, software, application and business processes. In cloud computing resources are shared online because of which these systems are facing severe security problems. Since its inception, Cloud computing has achieved its pervasive demand in academia and industry. As a cloud is providing an ample number of facilities in a very effortless manner, so an enormous number of users are using many cloud-based services, which upsurge the data traffic in the network this causes various security challenges for example trust, availability, integrity, confidentiality and privacy[1].

** Author for correspondence*

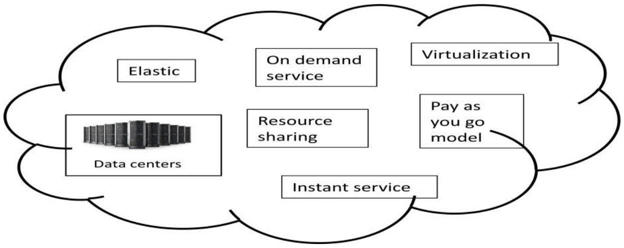

Figure 1. Cloud computing environment.

There are five essential characteristics of cloud computing, namely on-demand self-service, broad network access, rapid elasticity, resource pooling, measured services and because of these characteristic also shown in Figure1.Cloud computing can provide tremendous services in a very comfortable and convenient manner. The user can increase or decrease the resource according to their usage and will have to pay only for the used resources. Cloud computing comprises of different layers, relying on the dispensation of the resources. Based on this Memory, CPU, and other hardware components reside at the bottom most layer, called as Infrastructure as a Service (IaaS) layer. The middle layer Platform as a Service (PaaS) is responsible for hosting various environments for customer specific services. The top most layer is known as Software as a Service (SaaS) layer, from where the user can access cloud through a web service and web browsers. An example of SaaS is salesforce.com, and Amazon EC2 is an example of IaaS and Google app engine is an example of PaaS. The cloud can be deployed as public cloud, private cloud, hybrid cloud and community cloud.

Having all aforementioned characteristics and flexibility, cloud computing has to deal with many security challenges. When multiple users share data and resources, there is a risk of data misuse and various attacks. Protection of data and resources is the biggest challenge in cloud computing. The main security challenges in cloud computing are Confidentiality, integrity, and availability. Out of these three mentioned security challenges availability is causing a significant effect on the cloud environment. Cloud is well known for the availability of resources in a pool which can be used by the clients at any time. DDoS attack is a type of attack which harnesses the availability of resources by engaging them in malicious requests, because of which the benign user are not able to use the resources, which affects the liability of the provider and cause the loss of faith by the customer. So a proper mitigation technique is required to overcome the DDoS attack. So that the benign user can use the resources uninterruptedly.

The paper is organized as the Section I gives the introduction to the Cloud computing environment and its security issues. Section II describes the DDoS attack and its classification and various types of DDoS attack. In section III, we had mentioned the mitigation techniques, classification and different mitigation techniques used in the various papers. Section IV presents the proposed mitigation scheme and Section V ends with the overall conclusion.

2. DDoS Attack

As the resources shared in cloud computing are through the internet, so it is facing various security issues like security, Authentication and different kinds of attacks. DDoS is one of the most dangerous attacks causing unavailability of resources to benign uses. DDoS attack is conducted by one or more compromised systems which work under the control of the attacker. The main idea of the attack is to flood the predetermined target to make its resources unavailable to the benign users. The attacker takes control over some of the machines and makes them zombie machine, after having full control over these Zombie computers, the attacker launches the attack through these Zombie machines. The attacker sends the malicious request packet to the Zombie machines which forward those packets to target machine to consume all its resources. When a benign request comes for resource then it reflects the unavailability of resources[2].

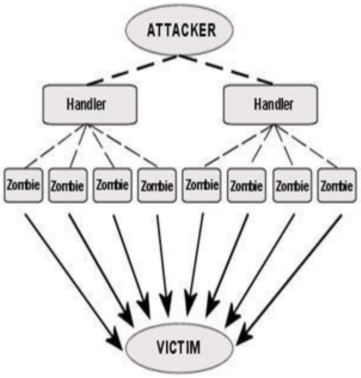

Figure 2. DDoS attack in cloud computing.

Hierarchy of conducting a DDoS attack in cloud computing is shown in Figure 2. It starts with an attacker node which controls the handlers, and the handlers inturns handle the zombie to launch the attack. The zombie machines generate lots of false request packets to overburden the target machine. DDoS attack significantly affects the various services of the network by consuming all resources and services by sending the malicious request. Distributed denial-of-service (DDoS) attacks pose a serious threat to network security. There are various tools which are being used by the attacker to launch the DDoS attack. These tools are Low Orbit Ion Canon (LOIC), XOIC, DDoSIM, DVOSET, PyLoris, HULK, R-U-Dead-Yet and Golden Eye and HTTP Dos Tool. All these are easily available on the internet and attacker can use any of the tools to launch the attack.

2.1 DDoS Attack Classification

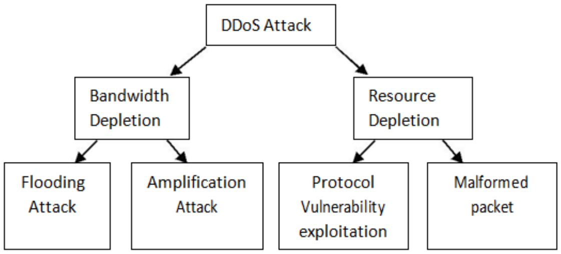

Figure 3. Taxonomy of DDoS attack [4].

Various researchers have given different classifications for the DDoS attack. In paper[4,5] describe the DDoS Classification as Infrastructural level and Application-bug level. Another classification for DDoS attack is mentioned in Paper[6] is based on Coercive Parsing, oversized payload, and flooding attack. In Paper[3] classified DDoS attack into bandwidth and resource depletion as shown in Figure 3.

2.1.1 Bandwidth Depletion Attack

In bandwidth depletion attack all the bandwidth available to the victim is consumed by the attacker by flooding the unwanted traffic to inhibit the benign traffic from approaching the target network. Many tools can be used to perform these attacks. The bandwidth depletion attack is further classified as:

2.1.1.1 Flood Attacks

This attack can be conducted by dispatching the large volume of traffic to the victim machine with the help of zombie machines managed by the handler. This huge amount of traffic floods the victim server and consumes all the bandwidth.

2.1.1.2 Amplification Attacks

This attack is launched by sending a large number of packets to broadcast IP address. In turn, it will send a reply to the victim system by the machines which are in the broadcast range. This kind of attack exploits the broadcast address feature found in most of the internetworking devices like routers. This attack can be launched by the attacker itself or can be started with the help of zombie machines also.

2.1.2 Resource Depletion Attacks

This type of attack is performed to impoverish the target machine system resources. As a result, the benign user is not able to use the resources. The following are the types of Resource depletion attacks:

2.1.2.1 Protocol Exploit Attacks

By exploiting the various features of the protocols installed on the target machine, an attacker can consume all the surplus resources. PUSH+ACK, TCP SYN, and CGI request are some of the examples of this type of attack

2.1.2.2 Malformed Packet Attacks

In this type of attack, the attacker sends the malformed packet wrapped with malicious data or information. The attacker sends this packet to the target machine to crash it. This can be done in two ways, either by IP address attack or by IP packet option attack.

3. DDoS Mitigation

There are various solutions presented by researchers for DDoS attack. We can implement the DDoS attack defense at different points. At first instance that is at the first interaction point, the attack can be prevented. Whenever the request arrives, a Turing test may help in preventing the attack. At the intermediate stage, the attack detection and prevention both can be done by various techniques. The third stage of defense can be implemented at the Victim site to mitigate and recover the system.

From all the three defense points we are focusing our interest towards DDoS attack mitigation. For any target machine if it has the sufficient resources to fulfill the attack requirements, then the attack will never be satisfied. Cloud providers have adequate resources to beat the DDoS attack. So the DDoS attack will never cause the cloud to be shut down. But the client-server or the cloud user does not have sufficient resources to overcome the attack.

Classification of DDoS Mitigation technique is shown in Figure 4. The mitigation techniques are classified as collaborative and non-collaborative[7]. The collaborative methods are further classified as Cooperative FWs, push back and back holing. The Non-collaborative techniques are classified as Static and dynamic. Dynamic techniques are further classified as redirecting and shunting and reconfiguration. Reconfiguration techniques are again further classified as service, network and defense.

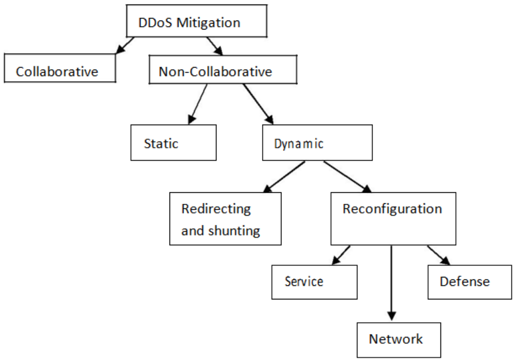

Figure 4. Classification of DDoS mitigation techniques[8].

Collaborative: In collaborative strategy, many nodes work together to mitigate the attack, and the victim get defended effectively. Multiple nodes cooperate to mitigate the DDoS attack and defend the victim effectively. The main three cooperative strategies to mitigate DDoS are Firewall, Pushback, and Blackholing.

Non-collaborative: These strategies involve many nodes, but there is no collaboration between these nodes for services, security appliances, or network elements. This strategy can be static or dynamic. Dynamic policy work like an adaptive model, here concerning the DDoS attack austerity defense architecture will be automatically adjusted by the mitigation mechanism. In contrast, in static approaches, the defense mechanisms are not adapted to the attack.

4. Literature Survey

Some of the mitigation techniques used in various papers are shown in Table 1. Further part of literature survey also shows some of the recent works done in this field.

In Paper[15] proposed a scheme that uses an IDS to detect DDoS attack by simulating Artificial Immune System (AIS). The system uses algorithm based on anomaly and signature based approach for the detection. The algorithm is mapped to AIS called "Generation of detector" to detect the attack. Whenever the attack is identified, a new

Table 1. Mitigation approaches used in different papers

S.No.	Technique Name	Mechanism	Limitation or Flaws
1.	Resource scaling[9,10]	With the most attractive feature of cloud "Resource scaling" provides a quick relief to resource bottleneck due to DDoS attacks. Keep serving the request with scaled resources. Now the victim machine can serve the clients even at the time of the attack.	False alarm may leads to EdoS. Co-hosted VMs may also be affected.
2.	Migration[11,12]	Migrating the DDoS victim server to another physical server which helps in minimizing losses. When the attack is detected and get mitigated then again migrate the server to its actual location.	The scheme may have migration cost and overhead.
3.	Backup resources[11]	The scheme uses dynamic resource allocation feature of the cloud and the victim server can use the additional resource to mitigate the attack.	Difficult to decide the number of backup resources. It may cause the heavy back up resource cost.
4.	Shutdown[13]	It is trivial and a quick way to mitigate the DDoS attack is to shut down the system. But it does not provide any solution to DDoS attack and may cause the benign user to suffer the down-time.	Because of the down time Business, reputation and long term business effects.
5.	Software defined network[14]	It is an emerging network paradigm which can reconfigure. It separates the data and control plane to support network reconfigurability. Are also supports the ISP-level monitoring of traffic.	Many legitimate requests get also suffered.
6.	Third party mitigation[15]	DDoS protection can be done on servers or on intermediate nodes which forwards packets to the server. As there are not many products to mitigate the DDoS attack directly. So a third party can be used to mitigate the server.	Extra expenses caused for the maintenance of third party

generation is added to dataset. The proposed method had high accuracy and correctness. The proposed solution efficiently reduces the false positive and increases the detection rate.

A Model based on Machine learning approach has been used in paper[16], which is used for the early detection of App-DDoS in a very fast manner. The Re-quest chain length, request chain context, ratio of packet types, ratio of packet count, route context, router chain context and ratio of request intervals are set of metric defended by the proposed model. The unique ness of the model is that it uses the set of request to identify the anomalies. The proposed model is significant in App-DDoS attack detection with crowded request of petabytes.

In Paper[17] author uses the anonymity provided in the internet by which they proof themselves as benign users and sends the fake messages to the users. The proposed model is for analyzing the email content and mitigating the phishing attack. Using the properties of hyperlinks, a server side algorithm is proposed for server side anti phishing email add-on. This algorithm provides a way to mitigate email phishing.

In paper[18] proposed a DENFIS algorithm for detection ICMPv6 Flood Attack. In this method they send the ICMPv6 flood attack packets using the application developed in C#. the packets were generated with different attack rates varying from 1000 pings to 1500 pings. It also generates the normal traffic with rates lying between 10 pings to 15 pings. The data set is divided into two sets i.e. 80% for training and 20 % for testing. It is proved in the paper that ICMPv6 flood attack can be detected with low root mean square error which is about 0.26.

In paper[19] proposed a prototype for detecting the attack. It retrieves the background information using SNMP. The data recovery can be done by other device using SNMP, by maximizing the available processing power for switching and routing. During the detection a source IP address is produced and it is blacklisted and is added to firewall to block the traffic from that IP address.

5. Proposed Work

To overcome the DDoS attack, there are basically three solutions Prevention, detection, and mitigation. Out of these three attack mitigation is the easiest way for the DDoS attack solution. In the proposed solution a list of faulty IP addresses has been prepared based on their performance during the Turing test and named as the blacklist. An IP address is called a faulty IP address if it is not able to pass the Turing test or in the previous history that IP address is taking a long time to answer the question asked during the Turing test. So if the request made by the sender with the IP address in the black list, the system will not allow accessing the resources and drop its request. If the request will be passed through the first stage then at second stage it is checked weather the number of requested resources are less than the available resources or not. If available resources are greater than the number of requested resource than request will be passed to the third stage, otherwise it will ask for more resources to serve the request. At the third stage requesting an amount of resources are compared with a threshold value "Th". "Th" is the threshold value of the request that can be made maximum at time T. "Th" can be calculated by watching the behavior of a maximum number of requests made when there is no attack. If the request for the resource is less than "Th" then the resources will be allocated to the request otherwise this request will be dropped and suspected as the malicious request.

Figure 5 shows the flow chart for the proposed algorithm.

5.1 Flowchart

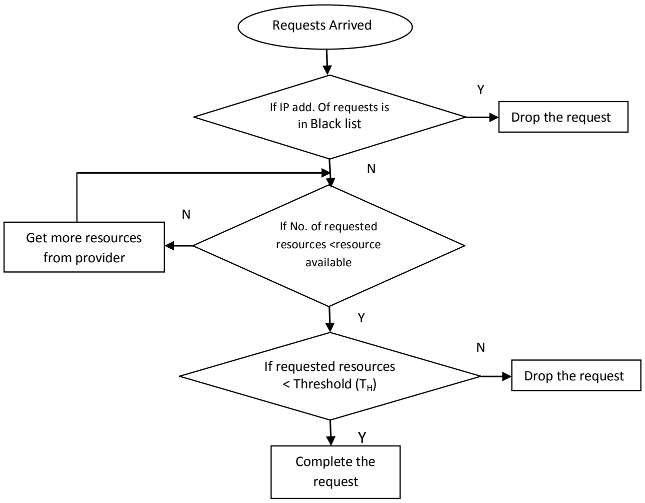
Requests Arrived
If IP add. Of requests is in Black list
Y
Drop the request
N
N
Get more resources from provider
If No. of requested resources <resource available
Y
N
If requested resources < Threshold (T_H)
Drop the request
Y
Complete the request

Figure 5. Flow chart for proposed DDoS attack mitigation algorithm.

5.2 Proposed Algorithm for DDoS Attack Mitgation

```
Step I: { If IP address of Requests at time T is in black list
Then drop the request
Step II: Else
{ If (Resource available at time T > Requested resources at time T)
Step III: { If (Requested resources < Threshold value of number request TH made at time T)
Step IV:  Then complete the requests
Step V: Else Drop the request}
Step VI: Else Ask for more resources from the provider
Step VII: After allocation of more resources goto II
```

- Whenever the number of requests arrives at time 'T', the IP address of these request falls into the blacklist or not. IF the IP address of request falls into the black list it will be suspected as malicious request and dropped.
- For the rest of the requests they check for weather the resources available are greater than the number of resources required by requests at time T. If yes, then GOTO step 3
- Then again, these requests are being checked for weather the resources requested are less than the threshold value for number of requests can arrive for a resource at time T.(if no then GOTO step 6)
- If yes the complete all the requests from different clients.
- If the number of requests is greater than the threshold value, then discard all the request.
- Ask for adding the more resources from the providers
- After allocation of more resources Goto step 2

6. Conclusion

In the last few years, there is a great increase in the number of DDoS attacks reported, because of the open nature of the cloud it is bared open to DDoS attack. Many researchers had focused on the detection of the DDoS attack based on Anomaly detection or signature based detection. But because of the repetitive occurrence of the DDoS attack, it has shown the limitation of the Attack detection mechanism. The new aspects have been embraced by academic research. This paper has presented the complete survey of mitigation approaches as well as proposed a mitigation technique to overcome the DDoS attack with minimum overhead.

7. References

1. Zissis D, Dimitrios L. Addressing cloud computing security issues. Elsevier Future Generation Computer Systems. 2012; 28(3):583–92.
2. Osanaiye O, Choo K. DDoS Resilience in cloud: Review and conceptual cloud mitigation framework. Journal of computers and network ap-plications, Elsevier. 2016; 67:147–65.
3. Deshmukh RV, Devadkar KK. Understanding DDoS attack & its effect in cloud. Environ Procedia Comput Sci. 2015; 49:202–10.
4. Wong F, Tan CX. A survey of trends in massive DDoS attacks and cloud-based mitigations. Int J Netw Secur Appl (IJNSA). 2014; 6(3):57–71.
5. Bhuyan MH, Bhattacharyya DK, JKalita JK. An empirical evaluation of information metrics for low-rate and high-rate DDoS attack detection. Pattern Recogn Lett. 2015; 51:1–7.
6. Cha B, Kim J. Study of multistage anomaly detection for secured cloud computing resources in future internet. In: Proceedings of IEEE Ninth International Conference on Dependable, Autonomic and Secure Computing (DASC), Sydney, Australia, Sydney, NSW. 2011. p. 1046–50.
7. Alireza S, Makan P, Fekih A. Taxonomy of Distributed Denial of Service mitigation approaches for cloud computing. Elsevier Journal of Network and Computer Applications. 2015; 58:165–79.
8. Mao MJLI, Humphrey M. Cloud auto-scaling with deadline and budget constraints. 11th IEEE/ACM International Conference on Grid Computing (GRID). IEEE, Brussels. 2010. p. 41–8.
9. Sarra A, Rose. DDoS Attacks in Service Clouds. In 48th Hawaii International Conference on System Sciences. IEEE Computer Society, USA. 2015. p. 5331–40.
10. Zhao K, Chen C, Zheng W. Defend against denial of service attack with VMM. Eighth International Conference on Grid and Cooperative Computing, GCC'09. IEEE, Malaysia. 2009. p. 91–6.
11. Latanicki J, Massonet P, Naqvi S, Rochwerger B, Villari M. Scalable Cloud Defences for Detection, Analysis and Mitigation of DDoS Attacks. In Future Internet Assembly. 2010; 127–37.
12. Wang H, Jia W, Dan F, Walter P, Li F, Angelos S. A moving target DDoS defence mechanism. Computer Communications. 2014; 46:10–21.
13. Rishikesh S, Gregory B, Zonghua Z. Towards Autonomic DDoS Mitigation using Software Defined Networking. SENT. 2015; 15(1):1–4.
14. HKhor K, Nakao A. Spow: On-demand cloud-based EDDoS mitigation mechanism. In Hot Dep (Fifth Workshop on Hot Topics in System Dependability), Tokya. 2009; 1–6.
15. Mueen U, Alsaqour R, Abdelhaq M. Intrusion Detection System to Detect DDoS Attack in Gnutella Hybrid P2P Network. Indian Journal of Science and Technology. 2013 Feb; 6(2):4045–57.

16. Munivara KP, Mohan AR, Venugopal RK. Anomaly based Real Time Prevention of under Rated App-DDOS Attacks on Web: An Experiential Metrics based Machine Learning Approach. Indian Journal of Science and Technology. 2016 Jul; 9(27):1–10.
17. Kumar JD, Srikanth V, Tejeswini L. Email Phishing attack mitigation using server side email addon. Indian Journal of Science and Technology. 2016 May; 9(19):1–5.
18. Saad RAA, Almomani A, Altaher A, Gupta BB, Manickam S. ICMPv6 Flood Attack Detection using DENFIS Algorithms. Indian Journal of Science and Technology. 2014 Jan; 7(2):168–73.
19. Mahmoudreza T. Immediate Detection of DDoS Attacks with using NetFlow on Cisco Devices IOS. Indian Journal of Science and Technology. 2016 Jul; 9(26):1–7.