Mitigation of DDoS Attacks in Cloud Computing

Preeti Daffu
P.G Student
P.G Student: Information Technology, CGC (Landran)
Morinda, India
preetidaffu461@gmail.com

Amanpreet Kaur
Assistant Professor
Professor: Department of IT, CGC (Landran)
Mohali, India
cecm.cse.akb@gmail.com

***Abstract*— Cloud computing provided its users with the more convenient way to use the resources and with a model where the users are charged as per the usage of their resources. The model is known as "pay-as-per- usage". Users can access the cloud services from anywhere at any time. They only need a working internet connection. Despite of all these benefits, cloud comes with some drawbacks also. The issue related to security of cloud is a biggest concern today. The attackers and hackers flood the network with attack packets and these are hard to identify as everything present on cloud is in virtual form. DDoS (Distributed Denial of Service) is a cloud-specific attack in which attack source is always more than one; multiple machines attacks on a user by sending packets with large data overhead. Such attacks make the resources unavailable to the user by overwhelming the network with unwanted traffic. In this research paper the main aim is to filter out the data packets with large data overhead to avoid DDoS attack and the Mean Time to Security Failure (MTSF) will be calculated so that an alternative dynamic plan can be adopted.**

Keywords— Distributed Denial of Service (DDoS); Mean Time to Security Failure (MTSF)

I. Introduction

Cloud computing provides its users to access the various cloud services and enables them to access the data storage and the computational resources with low data overhead. Cloud computing is rapidly growing and it has attracted the users to cloud. It offers the users to outsource the data resources from the remote locations when they need them. Cloud computing model has three effective service models and deployment models. The main characteristics provided to cloud users are: on demand service to its users, broad network access, resource pooling, rapid elasticity and measured service [5].

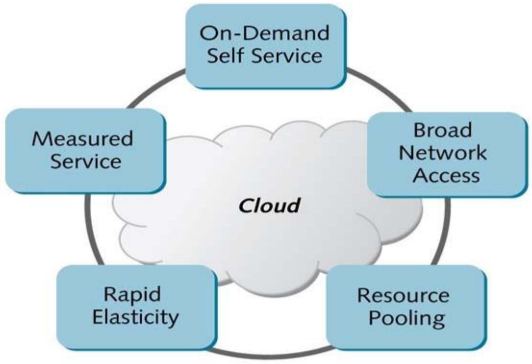


Fig. 1. Essential characteristics of cloud computing.

Cloud platform has provided its users to access the shared resources whenever they need i.e. on demand access. In cloud environment large pool of resources are available and these are allocated dynamically among its users. Cloud computing has gained an immense popularity by allowing its users to lease the computer resources when they run out of them, a pay-based usage of resources and this is known as "pay-as-you-use". It allows its users to run the applications directly from the cloud [7]. Today protecting the stored data on the cloud platform is an important issue that cannot be understated. Protecting the cloud from various attacks and their adversarial effects is a major concern that has stalled many users from shifting their data to the cloud.

The cloud infrastructure is fully virtualized and it supports all type of hardware architectures. Thus providing security to cloud is an important issue these days. The papers [4] [6] [7] give a clear idea about the security issues related to the cloud environment. Cloud is prone to a variety of attacks such as malware injection attack, Spoofing attack, flooding attack, DoS, DDoS and EDoS attack. Detection of the attack packets and filtering them to save the cloud users is a difficult task. Denial of service attacks made the sources unavailable to cloud users. Such attacks target the network bandwidth of the target user. Distributed Denial of Service (DDoS) attack is attempted to multiple users by flooding the packets. DDoS attacks are the most serious type of the network attacks.

DDoS Attacks: DDoS is a killer application for cloud computing environments on Internet today. It is a Distributed Denial of Service. We can beat the DDoS attacks if we have the sufficient resources. But the client-server and peer to peer system don't have the sufficient resources to beat them. Dynamic resource allocation strategy is used to counter the DDoS attacks. However cloud is still vulnerable to various attacks because cloud platform still runs its services in a traditional manner.

To prevent DDoS attacks, filtration of attack packets is needed. Dynamic allocation should be done to employ the idle resources to the cloud users and guarantee them with the quality of service. The main issue behind DDoS attacks is the competition between the resources. Only that side (attacker or user) which have more resources will win the battle. The side (attacker or user) which have more resources will win the battle. Botnets are used to carry out the various attacks such as

978-1-5090-0893-3/16/$31.00 ©2016 IEEE

DDoS attacks. The issue behind DDoS attack is resource management problem.

DDoS attacks are attempted in various forms, it can be flooding the network with a large amount of packets, synchronization of those packets or attackers may create the zombies towards the victim machine. The most basic and effective DDoS attack strategy is to flood the network with the attack packets. DDoS attacks have always been a threat to individual cloud customers as they have fewer resources to beat such attacks. But it is possible to mitigate the cloud attacks using various hazards of cloud computing.

A Denial-of-Service attack (DoS attack) makes the cloud resources unavailable or exhausts the resources for the cloud users. The common method used in such attacks is to saturate the network of the targeted machine with fake packet requests so that legitimate traffic on the network couldn't be responded. Such attacks usually overload the server. Distributed attacks involve the countless attackers who target a single machine.

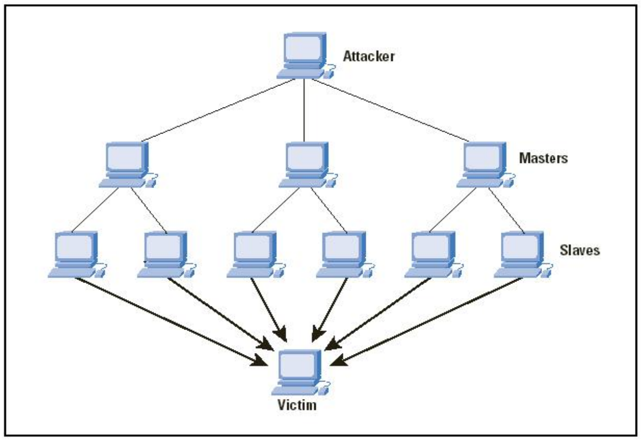


Fig. 2. A typical DDoS attack.

II. Related Work

DDoS attack mainly aims to flood the network of the cloud user with attack packets and to make the resources unavailable to its users. Earlier the DDoS attacks were detected in the year 2000 and the most of the well known sites were targeted by the hackers such as Amazon, Yahoo. Earlier these attacks were just for the purpose of the curiosity and fun. Then there was rapid increase in cyber attacks due to a huge financial and the potential rewards available to the cloud hacker [1]. Distributed Denial of Service (DDoS) attack is a major security concern for all the internet based applications and in cloud environments also [2]. The data is saved on the internet, instead of the hard disk of the computer. Botnets are majorly used to carry out the DDoS attacks.

In [3] authors have described that authors can easily attack the computers as many they want to attack. The number of active bots that a botmaster can have is upto thousand levels and it is just because of antivirus and anti malware software. Recent researches [4], [5], [6] authors have described the essential issue related to the cloud computing and it is DDoS attack. It includes the competition for the resources between user and the attacker. The one side who has the more resources than others will win the battle.

Morein, William G. et al. (2003) has proposed the method to counter the ddos attacks using graphic turing tests against web servers. The authors have discussed robust technique based on the overlay architecture and it helps to grant the access to those web servers that have been targeted by the attacker for the denial of service attack. This model has used the two characteristics: human centric interface and the applets. Zunnurhain, Kazi. et. al. (2010) has analyzed the security attacks and their effects on the cloud. The authors have also proposed the solutions to such attacks. Cloud platform offers great potential and reduction in the cost and it is vulnerable to various threats and security risks. The authors have identified the possible security attacks on clouds including wrapping attacks, Flooding attacks, Browser attacks, accountability checking problems and malware injection attacks. Specific solutions were proposed and the root cause of such attacks was identified.

Bhandari, Nisha H. et. al. (2012) has conducted a survey on DDoS attacks, its detection and the defense approaches for such attacks. Nowadays DDoS attacks have become a serious threat to the cloud users and the buzzing technology. Distributed Denial-of-Service (DDoS) attack is a serious problem because such an attack is very hard to detect, there is no comprehensive solution and it can shut an organization business off from the Internet. The primary goal of an attack is to deny the victim's access to a particular resource. The authors have reviewed the current DoS and DDoS detection and defense mechanism.

III. Challenges In Existing Models

While cloud computing comes with various advantages and the benefits to its users and IT enterprises; it also has various drawbacks. Virtualization technology is backbone of the cloud environment. Cloud provides its users with a lot of advantages such as easy and dynamic allocation of the cloud resources, space and the cost reduction. But security related issues of cloud still keep away the plenty of users from using the cloud computing technology. They still hold on to their traditional technology. Chances of cross channel attacks have been increased due the existence of techniques that can physically locate the virtual machines. It has increased the chances of data loss during the transmission. So, this work proposed a framework to counter such attacks. The existing model was a queuing theory model that has been established to eliminate the resource allocation against various attacks. Careful data analysis and real world data set experiments helps to beat DDoS attacks at affordable costs.

Problem Formulation: In proposed model chances of occurrence has been checked and the DDoS attacks are mitigated on basis of these chances. In the proposed model Mean Time to Security Failure (MTSF) will be calculated and a dynamic mitigation plan will be adopted. It improves the trust of customer on enterprises using cloud platform. A security layer has been added to provide the cloud solutions. Whenever there is a risk of a DDoS attack, it can be mitigated by calculating its mean time to security failure and then adopting an alternative plan. Whenever there are packets on the network with a large data overhead then it will filter out such packets and identify those packets as DDoS attack.

IV. Methodology

In proposed model the tool used to beat the DDoS attacks is CloudSim i.e. Cloud Simulation Tool. It is an open source tool. It has simulation kit for cloud computing scenarios. Cloud Simulation tool is always implemented in Java. This tool includes basic classes for describing data. To work with this tool basic Java programming is needed and basic knowledge about cloud computing. Java programming environment is needed to work with the CloudSim; it may be Eclipse or Netbeans. By using CloudSim, industry-based developer's and researchers can identify the low level details related to cloud services and the cloud based infrastructures.

The algorithm used here is to calculate the mean time to the security failure i.e. MTSF. This algorithm will helps us to calculate the mean time that an attack may need to get on the destination computer. From this calculated value a new dynamic alternative plan may be adopted so that attack is prevented before it occurs. The mechanism used to beat the DDoS attacks is preventive mechanism which involves the prevention of the attacks before they occur.

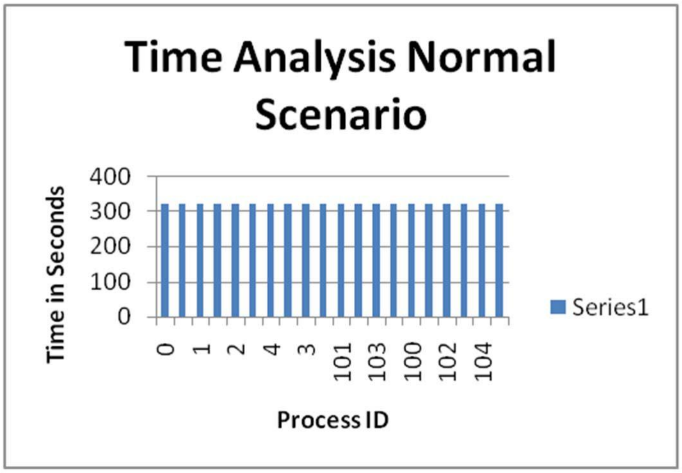
The Procedure followed is: The steps to be followed to mitigate a DDoS attacks or to reduce them are as follows:

1. The start and finish time of the packets is checked by running the normal command.
2. The packets having the large data overhead are detected as the attack packets and are filtered out if they are from the unknown sender.
3. MTTSF (mean time to security failure) is calculated and then alternative dynamic plans adopted to mitigate those attacks.
4. The attacks packets are filtered out at the end.

V. Experimental Results

The proposed model has used the various parameters and the results are shown below. The performance evaluation has been performed on the basis of accuracy of the system to offloading the processes.

Graph 1: In this graph normal scenario has been analyzed for its performance by processing the 20 processes over the given cloud configuration. The normal scenario have resulted in 320 seconds for the given process list. The homogeneous process list has been tested under this testing process.



Graph 1: Time based analysis for normal scenario

Table 1:

CLOUDLET ID	FINISH TIME	TOTAL TIME
0	320.1	320
1	320.1	320
2	320.1	320
4	320.1	320
3	320.1	320
101	320.1	320
103	320.1	320
100	320.1	320
102	320.1	320
104	320.1	320
109	520.1	320

Table 1: normal scenario results

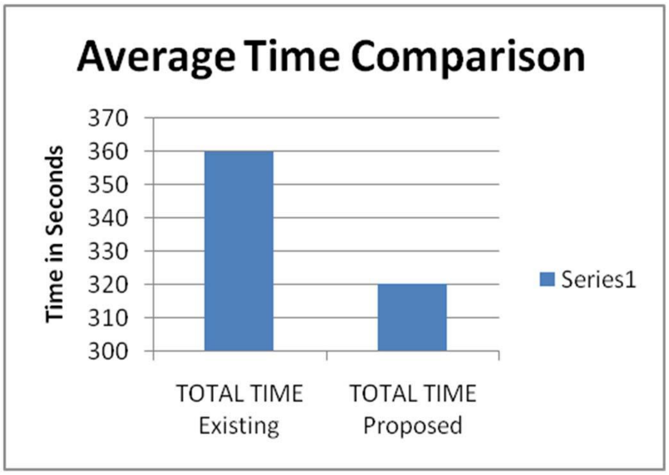
Table 2: The DDoS attack scenario has been designed by simulating the 5 attacker nodes for the purpose of DDoS attack simulation. The cloud has been analyzed for its performance by processing the 20 processes over the given cloud configuration under the attack situation. The attack scenario has resulted in 360 seconds of process length for every given process in the process list.

CLOUD LET ID	START TIME	FINISH TIME	TOTAL TIME	DATA OVER HEAD
0	0.1	360.1	360	100000
5	0.1	360.1	360	100000
1	0.1	360.1	360	100000
6	0.1	360.1	360	100000
2	0.1	360.1	360	100000
7	0.1	360.1	360	100000
4	0.1	360.1	360	100000
9	0.1	360.1	360	100000
3	0.1	360.1	360	100000
8	0.1	360.1	360	100000

101	200.1	560.1	360	100000
106	200.1	560.1	360	100000
103	200.1	560.1	360	100000
108	200.1	560.1	360	100000
100	200.1	560.1	360	100000
105	200.1	560.1	360	100000
102	200.1	560.1	360	100000
107	200.1	560.1	360	100000
104	200.1	560.1	360	100000
109	200.1	560.1	360	100000

Table 2: Table of Attack scenario of data packets.

Graph 2: The graph has shown the comparison between the time of existing and proposed model. Both scenarios have resulted in the form of overall processing time for each process while tested over the DDoS attacks. The security model with authentication offers the elapsed time of 320 and the other model without authentication has resulted in average elapsed time of 360 seconds process length for every given process in the process list.



Graph 2: Average time based comparison for each process in the job list.

Table 3: This table shows the values for the existing model. This table shows that the time overhead has been reduced from 40 to 0. It is the value of time taken by each process to execute in the process list. The value of time overhead has shown improvement as compared to the existing model.
Existing technique Values:

CLOUD LET ID	TOTAL TIME	TIME OVERHEAD	DATA OVERHEAD
0	360	40	100000
5	360	40	100000
1	360	40	100000
6	360	40	100000
2	360	40	100000
7	360	40	100000
4	360	40	100000

Proposed technique Values:

CLOUD LET ID	TOTAL TIME	TIME OVERHEAD	DATA OVERHEAD
0	320	0	1000
5	320	0	1000
1	320	0	1000
6	320	0	1000
2	320	0	1000
7	320	0	1000
4	320	0	1000

VI. Conclusion

DDoS attacks are shutting down the cloud services and also putting a huge burden on cloud users. The loss to the cloud users can be economically or financially. Cyber criminals use such attacks as a tool to hurt the cloud users. It is concluded that DDoS attacks can be countered by dynamic allocation of the resources. A strategy is used to provide the cloud users with the quality of service and to mitigate the DDoS attacks by calculating the mean time.

Acknowledgment

I acknowledge with deep sense of gratitude and most sincere appreciation, the valuable guidance and unfailing encouragement rendered to me by “Mrs. Amanpreet Kaur” Assistant Professor for their proficient and enthusiastic guidance, useful encouragement and immense help. I have been deep sense of admiration for them inmate goodness and inexhaustible enthusiasm. The proposed work will be completed under the guidance of the official guide and other experts at the campus of the Chandigarh group of Colleges, Landran, and Mohali.

References

[1] B. Stone-Gross, M. Cova, L. Cavallaro, B. Gilbert, M. Szydlowski, R. Kemmerer, C. Kruegel, and G. Vigna, “Your botnet is my botnet: Analysis of a botnet takeover,” in Proceedings of the 2009 ACM conference on computer communication security, 2009.
[2] T. Peng, C. Leckie, and K. Ramamohanarao, ‘‘Survey of Network-Based Defense Mechanisms Countering the dos and ddos Problems,’’ ACM Comput. Surv., vol. 39, no. 1, pp. 1-3, 2007.
[3] M.A. Rajab, J. Zarfoss, F. Monrose, and A. Terzis, ‘‘My Botnet is Bigger Than Yours (Maybe, Better Than Yours): Why Size Estimates Remain Challenging,’’ in Proc. 1st Conf. HotBots, 2007, p. 5.
[4] S. Yu, S. Guo, and I. Stojmenovic, ‘‘Can We Beat Legitimate Cyber Behavior Mimicking Attacks from Botnets?’’ in Proc. INFOCOM, 2012, pp. 2851-2855.
[5] Y. Chen, K. Hwang, and W.-S. Ku, ‘‘Collaborative Detection of ddos Attacks over Multiple Network Domains,’’ IEEE Trans. Parallel Distrib. Syst., vol. 18, no. 12, pp. 1649-1662, Dec. 2007.
[6] J. Francois, I. Aib, and R. Boutaba, ‘‘Firecol, a Collaborative Protection Network for the Detection of Flooding ddos Attacks,’’ IEEE/ACM Trans. Netw., vol. 20, no. 6, pp. 1828-1841, Dec. 2012.

[7] Can we beat DDoS attacks: - Published in:-Parallel and Distributed Systems, IEEE Transactions on (Volume:25 , Issue: 9), Date of Publication :24 July 2013. Author: Shui Yu, Senior Member, IEEE, Yonghong Tian, Senior Member, IEEE,Song Guo, Senior Member, IEEE, and Dapeng Oliver Wu, Fellow, IEEE

[8] Mitigating DDoS Attacks with Transparent and Intelligent Fast-Flux Swarm Network:- Published in: Network, IEEE (Volume:25 , Issue: 4), Date of Publication : July-August, 2011. Author: Ruiping Lua and Kin Choong Yow, Nanyang Technological University.

[9] Security Attack Mitigation Framework for the Cloud:- Published in: Reliability and Maintainability Symposium (RAMS), 2014 Annual , Date of Conference: 27-30 Jan, 2014. Author: Esha Datta, , Indian Institute of Technology, Neeraj Goyal,, Indian Institute of Technology

[10] An Unsupervised Approach for Detecting DDoS Attacks based on Traffic Based Metrics:- Communications, Computers and signal Processing, 2005. PACRIM. 2005 IEEE Pacific Rim Conference. Date of Conference: 24-26 Aug, 2005.

[11]Bhandari, Nisha H. "Survey on DDoS Attacks and its Detection & Defence Approaches." International Journal of Science and Modern Engineering (IJISME) ISSN: 2319-6386, vol 2, issue 7, July 2013.

[12]Morein, William G., et al. "Using graphic turing tests to counter automated ddos attacks against web servers." Proceedings of the 10th ACM conference on Computer and communications security. ACM, 2003, pp.08-19.

[13]Zunnurhain, Kazi, and S. Vrbsky. "Security attacks and solutions in clouds."Proceedings of the 1st international conference on cloud computing. 2010