ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 15, March 2016

DETECTION OF STEALTHY DENIAL OF SERVICE ATTACK FOR EFFECTIVE RESOURCE SHARING IN CLOUD COMPUTING

M.Elaiyaraja [1]
Department of Computer Science and Engineering
Dhaanish Ahmed College of Engineering,
Padappai, Chennai – 601 301
elaiyaraja1@gmail.com

Mr.K.Rajesh Kambattan, M.E.,(Ph.D)., [2]
Assistant Professor
Department of Computer Science and Engineering
Dhaanish Ahmed College of Engineering,
rajeshkambattan.k@dhaanishcollege.in

Abstract - The success of the cloud computing paradigm is due to its on-demand, self-service, and pay-by-use nature. According to this paradigm, the effects of Denial of Service (DoS) attacks involve not only the quality of the delivered service, but also the service maintenance costs in terms of resource consumption. Specifically, the longer the detection delay is, the higher the costs to be incurred. Therefore, a particular attention has to be paid for stealthy DoS attacks. They aim at minimizing their visibility, and at the same time, they can be as harmful as the brute-force attacks. They are sophisticated attacks tailored to leverage the worst-case performance of the target system through specific periodic, pulsing, and low-rate traffic patterns. In this paper, the impact of DDoS attack in cloud environment is analyzed and used mIPS to avoid DDoS attack, as per the client server environment is concerned, DDoS attack would collapse the entire system but as far as Cloud is concern, DDoS attack would make the cloud resource to be not available for end cloud user, to avoid DDoS attack, in this project, multiple Intrusion Prevention System (mIPS) techniques would be implemented and deployed to monitor the activity of the users and filters the request based on the behavior and forwards to the corresponding servers through Cloud Server. The user activities monitoring is done using mIPS and that would help to detect the DDoS attack faster and make the Cloud resource to be available to end cloud user. KDD CUP `99 dataset was used to analyze the patterns of user behavior to avoid the DDoS attack in cloud.

Keyword – Denial Of Service, Multiple Intrusion Prevention System, Cloud Computing, Attack Detection.

I. INTRODUCTION

Cloud infrastructure provider pools a large amount of resources and makes them easy access in order to handle a rapid increase in service demands [1]. Therefore, it is almost impossible for a DDoS attack to shut down a cloud. However, individual cloud customers (referred to as parties hosting their services in a cloud) cannot escape from DDoS attacks nowadays as they usually do not have the advantage. The good news is that it is highly likely for individual cloud customers to win the battle by taking advantage of the unique features of clouds. In this paper, I explore how to overcome DDoS attacks against individual cloud customers from the resource competition perspective. Currently, cloud computing has become one of the fastest growing sectors in the IT industry all over the world. Cloud

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 15, March 2016

computing features a cost-efficient, ''pay-as-you-go'' business model and flexible architectures, such as SaaS, PaaS and SaaS. A cloud platform can dynamically clone virtual machines in a very quick fashion, e.g., duplicating a gigabyte level server within one minute [2]. Despite the promising business model and hype surrounding cloud computing, security is the major concern for businesses shifting their applications to clouds [3], [4]. Distributed Denial of Service (DDoS) is a major threat to Internet based killer applications for non-cloud computing environments, such as independent news web sites, e-business and online games [13].

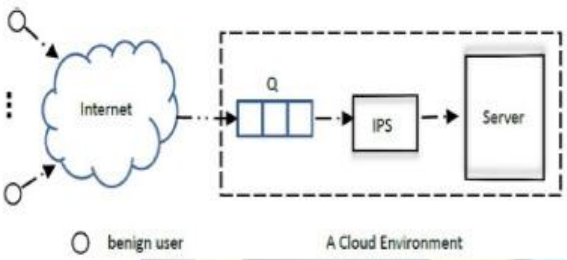

Fig 1. Cloud Architecture with Single IPS

The contributions of this paper are summarized as follows: I point out that DDoS attacks do threaten individual cloud customers. However, by taking advantage of the cloud platform, I can overcome DDoS attacks, which is difficult to achieve for non-cloud platforms. To the best of our knowledge, this paper is an early feasible work on defeating DDoS attacks in a cloud environment. I propose a dynamic resource allocation mechanism to automatically coordinate the available resources of a cloud to mitigate DDoS attacks on individual cloud customers. The proposed method benefits from the dynamic resource allocation feature of cloud platforms, and is easy to implement.

II. SYSTEM MODEL

The system architecture diagram shows how Multiple Intrusion Prevention System has been implemented and deployed in cloud environment to detect the denial of service attack in cloud environment. Usually, the user request are passed over the internet will be queued and send it to multiple intrusion prevention system as shown below and the request finally reaches Server. Here, the mIPS would monitor the end user activities and behavior to detect any potential attack is being initiated.

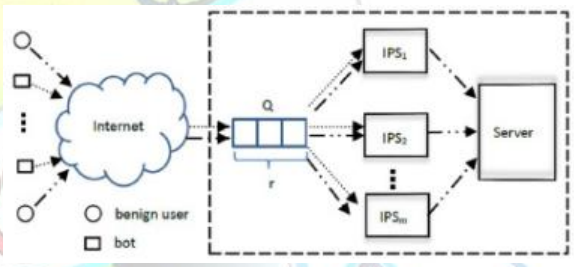

Fig 2. Cloud Architecture with Single mIPS

DDoS attack would make the cloud resource to be not available for end cloud user, to avoid DDoS attack, in this project, multiple Intrusion Prevention System (mIPS) techniques would be implemented and deployed to monitor the activity of the users and filters the request based on the behavior and forwards to the corresponding servers through Cloud Server. Based on user activities patterns, user behavior is monitored and DDoS attack is avoided in Cloud. The user activities monitoring using

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 15, March 2016

IPS would help to detect the DDoS attack faster and make the Cloud resource to be available to end cloud user. KDD CUP `99 dataset was used to analyze the patterns of user behavior to avoid the DDoS attack in cloud.

A. Cloud Server Deployment

Cloud Service Provider will contain the large amount of data in their Data Storage. Also the Cloud Service provider will maintain the all the User information to authenticate the User when are login into their account. The User information will be stored in the Database of the Cloud Service Provider. Also the Cloud Server will redirect the User requested job to the Resource Assigning Module to process the User requested Job. The Request of all the Users will process by the Resource Assigning Module. For this Purpose we are going to create an User Interface Frame. Also the Cloud Service Provider will send the User Job request to the Resource Assign Module in First In First Out (FIFO) manner. data storage; routing; and data processing.

B. Deployment of Multiple IPS

In this module we implement multiple IPS ie intrusion protection system that used to protect the user form the attacks .in existing they were using single to scan the query of a cloud user. but in this proposed module we multiple IPS is deployed to monitor the user query so that it easily find the denial of attack.

C. DDOS from Single User

This effectively makes it impossible to stop the attack simply by blocking a single IP address; plus, it is very difficult to distinguish legitimate user traffic from attack traffic when spread across so many points of origin.

D. Multiple User From Same IP

In this module multiple user will be login in the same IP address and send query so it will see the account and it will lead to overload on the sever. In out proposed we monitor the query coming from multiple user form the same ip .And we analysis IP address to find the DDOS attack.

E. Attacks Filtering Model

I present a probabilistic packet filtering (PPF) mechanism to defend the Web server against Distributed Denial-of-Service (DDoS) attacks. In the attack filtering model we implement the requested huge sized file beyond the permitted. Based on these patterns user behavior is monitored DDOS attack is avoided in cloud.

III.DEFINITIONS AND ASSUMPTIONS

A. DDoS Attack:

A distributed denial-of-service (DDoS) attack in cloud computing occurs when multiple systems flood the bandwidth or resources of a targeted system, usually one or more web servers/end users. Such an attack is often the result of multiple compromised systems (for example a botnet) flooding the targeted system with traffic.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 15, March 2016

B. Cloud Computing:

Cloud computing, also on-demand computing, is a kind of Internet-based computing that provides shared processing resources and data to computers and other devices on demand. It is a model for enabling ubiquitous, on-demand access to a shared pool of configurable computing resources. DDoS attack in cloud computing would affect the Service Level Agreement between Cloud service provider and end user. So, this paper is to how to detect such attacks in cloud computing.

C. Multiple Intrusion Prevention System:

Intrusion prevention systems (IPS), also known as intrusion detection and prevention systems (IDPS), are network security appliances that monitor network and/or system activities for malicious activity. In this paper, I have introduced mIPS to monitor user activities and behaviors in cloud computing to detect DDoS attackes.

IV. SYSTEM IMPLEMENTATION TO DETECT DDOS ATTACK

The proposed technique to implement Multiple Intrusion Prevention System (IPS) to Monitor the Activity of the Users and Filters the Request based on the behavior and forwards to the corresponding Servers through Cloud Server. Every Server would have allocated Certain Space in Cloud Server. IPS Monitors the Activity of the Users to Avoid DDoS Attacks

A. Space Allocation Phase For Each Server:

Cloud Servers is a cloud infrastructure service that allows users to deploy "one to hundreds of cloud servers instantly" and create "advanced, high availability architectures". Christo Ananth et al. [5] proposed a secure hash message authentication code. A secure hash message authentication code to avoid certificate revocation list checking is proposed for vehicular ad hoc networks (VANETs). The group signature scheme is widely used in VANETs for secure communication, the existing systems based on group signature scheme provides verification delay in certificate revocation list checking. In order to overcome this delay this paper uses a Hash message authentication code (HMAC). It is used to avoid time consuming CRL checking and it also ensures the integrity of messages. The Hash message authentication code and digital signature algorithm are used to make it more secure . In this scheme the group private keys are distributed by the roadside units (RSUs) and it also manages the vehicles in a localized manner. Finally, cooperative message authentication is used among entities, in which each vehicle only needs to verify a small number of messages, thus greatly alleviating the authentication burden.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 15, March 2016

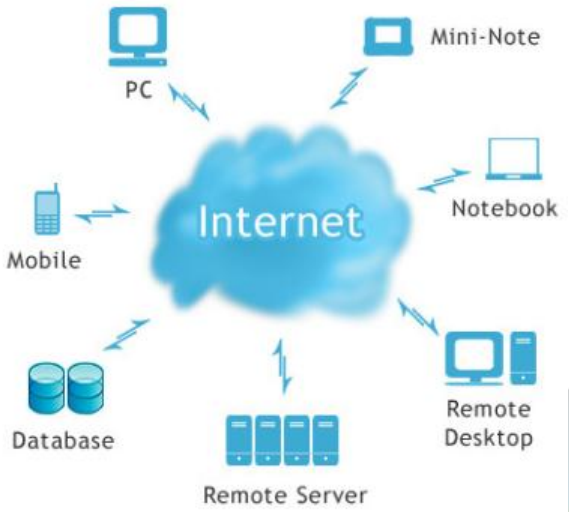

Fig 3. Space Allocation Process diagram

Fig.3. Shows how the space allocation is done for each server is created. Each server that are created will have specified size allocated to that.

B. Cloud Server Deployment Phase:

The Cloud Service provider will maintain the all the User information to authenticate the User when are login into their account. The User information and user authentication information will be stored in the Database of the Cloud Service Provider and also the User Requested jobs are redirected to Resource Assigning Module via the Cloud Server. The Resource Assigning Module will be used to process all user requests. To communicate with the Client and with the other modules of the Cloud Network, the Cloud Server will establish connection between them. For this Purpose I am going to create an User Interface Frame.

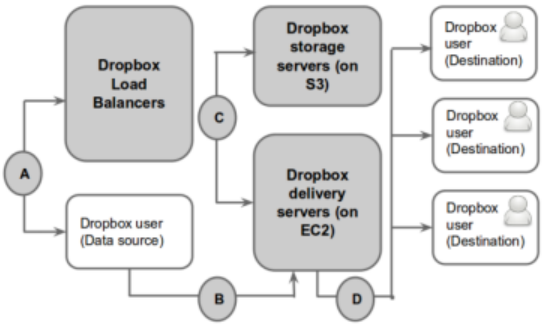

Fig 4. Deployment of Cloud Server.

In Fig.4, Shows how a cloud server has been created and how it can be accessed from our project to send the user request. We would be using Cloud Server App Key and App Secret Key for accessing the Cloud Server and to pass on the user requests.

C. Multiple IPS Creation and DDoS Detection Phase:

Implemented multiple IPS ie intrusion prevention system that used to protect the user form the attacks in existing they were using single and multiple users to scan the query of a cloud user. however, in this proposed module multiple IPS is deployed to monitor the single/multiple user query so that it easily find the denial of attack in the queries being sent to cloud server.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 15, March 2016

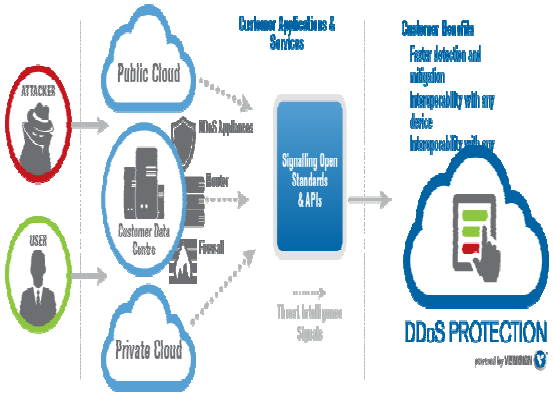

Fig 5. DDoS Attack Detection Diagram.

In Fig. 6 shows how multiple intrusion prevention system is created to monitor the end user activities and behavior and block the user once the specified user pattern is matched.

V. CONCLUSION

In this paper, I have pointed out that DDoS attacks are still an effective tool for cyber criminals to shut down individual cloud customers, even though it is almost impossible to deny the service of a cloud platform. At the same time, I also note that a cloud possesses a potential to counter this kind of brute force attack by using its profound resources and showed how the mIPS can be implemented and detect the attacks that are being sent to Cloud Server, this solution will help to maintain the Service Level Agreement signed between Cloud Service Provider and Cloud Service User.

VI. FUTURE SCOPE

I have motivated by this and I design a strategy to dynamically allocate idle or reserved cloud resources to those cloud customers who are experiencing DDoS attacks in order to defeat the attacks, and at the same time guaranteeing the quality of service for benign users. I establish a queueing theory based model for the proposed DDoS attack mitigation strategy in a cloud environment. I would thoroughly analyse the proposed method. Extensive real-world data set based experiments and simulations confirm our claim that I can beat DDoS attacks on individual cloud hosted services with an affordable cost to cloud customers.

REFERENCES

[1] M.Armbrust, A.Fox, R.Griffith, A.D.Joseph, R.H.Katz, A.Konwinski, G.Lee,D.A.Patterson,A.Rabkin, I. Stoica,andM.Zaharia, ‘‘Above the clouds: A berkeley view of cloud computing,’’ EECS Dept., Univ.California, Berkeley,CA, USA, Tech. Rep.UCB/EECS-2009- 28, Feb. 2009.

[2] C. Peng, M. Kim, Z. Zhang, and H. Lei, ‘‘Vdn: Virtual Machine Image Distribution Network for Cloud Data Centers,’’ in Proc. INFOCOM, 2012, pp. 181-189.

[3] S. Subashini and V. Kavitha, ‘‘A Survey on Security Issues in Service Delivery Models of Cloud Computing,’’ J. Netw. Comput. Appl., vol. 34, no. 1, pp. 1-11, Jan. 2011.

[4] R. Bhadauria, R. Chaki, N. Chaki, and S. Sanyal, ‘‘A Survey on Security Issues in Cloud Computing,’’ CoRR, vol. abs/1109. 5388, 2011.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 15, March 2016

[5]Christo Ananth, M.Danya Priyadharshini, "A Secure Hash Message Authentication Code to avoid Certificate Revocation list Checking in Vehicular Adhoc networks", International Journal of Applied Engineering Research (IJAER), Volume 10, Special Issue 2, 2015,(1250-1254)

[6] 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.

[7] D.K.Y. Yau, J.C.S. Lui, F. Liang, and Y. Yam, ''DefendingAgainst Distributed Denial-of-Service Attacks with Max-Min Fair Server- Centric Router Throttles,'' IEEE/ACM Trans. Netw., vol. 13, no. 1, pp. 29-42, Feb. 2005.

[8] S. Yu, S. Guo, and I. Stojmenovic, ''Can We Beat Legitimate Cyber Behavior Mimicking Attacks from Botnets?'' in Proc. INFOCOM, 2012, pp. 2851-2855.

[9] 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.

[10] 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.