ISSN: 0975-766X
CODEN: IJPTFI

Available Online through ***Research Article***
www.ijptonline.com

A SYSTEMATIC APPROACH TO DETECT AND DEFEND DDOS ATTACKS IN CLOUD

Dhinesh Babu L.D, Manoj Kumar V, Sathish Kumar T.C., Satheesh Kumar K
School of Information Technology and Engineering, VIT University, Tamil Nadu, India.
Email: lddhineshbabu@gmail.com

Received on 25-10-2016 *Accepted on 02-11-2016*

Abstract

Cloud computing delivers various services through the Internet, which meets the demands of different devices. Trending in different way cloud uses the concept of virtualization which drags different platforms, resources, software's,etc.into a single window. There are many services offered by a cloud like software- as- a service (SaaS), Platform- as -a service (PaaS), infrastructure as a service (IaaS) and Network- as -a service, Even though the benefits of these services are huge cloud suffers from various threats. In this paper, we mainly focus on the DDoS attacks in the cloud and provide a systematic approach to detecting and defend DDoS attacks in the cloud.

Keywords: Cloud computing, DDoS attack.

1. Introduction

Cloud offers various services through the internet which can be served to different machines. Services provided by the cloud enables us to work on different machines of various hardware and software configurations virtually. It also allows us to manage and store our data through different terminologies. One can run a program or a complicated software using his/her machine with lower configuration through the cloud. One can pay and use required software which may cost much less than buying the same software and installing them into the system. Still, there are various services provided by the cloud which iseffectively used by different companies and users. These services are grouped based on their specifications[1]. Fundamentally which are name as i) Software as a service. Ii) Infrastructure as a service. Iii)A network as a service. There are various issues in implementing these services effectively, for example, the different types of data are stored in different places of a single user in the cloud. The process of collecting it back forms the difficult task, and it grew more complex when large volumes of data are retrieved from different locations. However, the severity of these problems are too low hence it can be handled and resolved.

Cloud manager handles these tasks from accepting users to the withdrawal of assigned services. The benefits and usage of cloud services are enormous but security, privacy are serious threats in the cloud which form the highest severity[2]. Privacy is concerned with leakage of our confidential information or data where security is concerned with the hacking of our results or resources. Focusing on the safety issues, there are some threats to be resolved which may cause severe damage to a cloud provider or the user[3]. The greatestdanger is DDoS attack which acquires the services from the users.

2. Relatedwork

Distributed denial of service attack made on the cloud makes all services unavailable to the user[4].Moreover, the attacker holds full control of all the services and the data which spoils the main theme of the cloud. A DDoS Filtering Algorithm[5]was proposed by Yifu where the algorithm works based on the flow of IP, the disadvantage of this algorithm is it only detects IP floods of the same frequency. [5] Chu-Hsing focused on flooding attack by using Semantic Web concept, but this is restricted to identifying malicious browsing behaviors. Liming Al[6] proposed a system which requires data (IP address of hacker who made attack earlier), but in the cloud all cloud users or providers do not provide these information's and the system goes complex hence is based on Probabilistic Packet Marking Turner proposed a fuzzy logic which detects flooding attack. However, this logic goeswell with some systems where other suffered from false positive even though there is an attack.

Huan[7] proposed a mechanism which defends DDoS attacks in new forms which taps the network under-supply in a cloud substructure. The authors proposed a strategy to discover the swamping brokers by conceiving all the possible types of IP are faking. The strategy is founded upon the TCP SYN/ACK protocol couple considering packet information. The ongoing security threats in the Cloud Computing services [8-10] needs a new strategy to overcome the denial attacks. Considering all these and further papers,DDoS attack requires some time to crash the system or application. However,am elementary attack can replicate in the data center and causes huge damage to the application and other application including the hardware. On observing how DDOs attacks are made we come to a conclusion that the assault is made mainly by flooding/deluging large number of packets and other is by utilizing bandwidth extremely, by sending a huge volume of data. In the paper, we discuss an approach which can be used to defend and detect DDoS attacks in the cloud. Hence two kinds of approachesare made one are packet frequency must be analyzed based on the arrival rate, and another is to analyze the amount of data reaching the system.

3. Systematic Approach

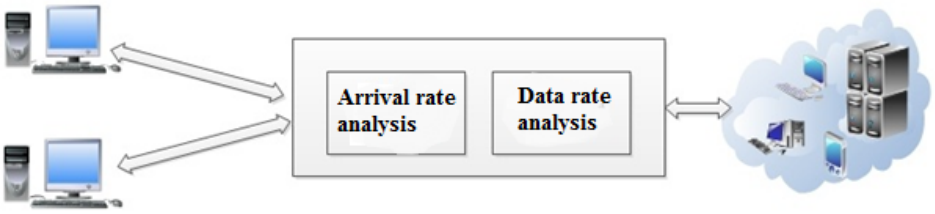

Figure 1: Analysis of the Data Packet.

The working of the system takes place in 6 steps:

(1) Estimation of Arrival Rate & Data Rate In Private Network:

The threshold value of both arrival rate and the data rate that is the maximum Arrival/Data rate the system can hold is estimated by using the private network. Hence a specific threshold value for both Arrival & Data is found.

(2) Arrival Rate Analysis:

The next step is to verify the incoming packet frequency with the threshold value which is found in the above step. I.e., the packet arrival r rate is verified with the threshold arrival rate which is determined by using the private network. In figure 2, the complete architecture of the work is shown.

(3) Flooding Attack Detection:

In the comparison of the data rate with the threshold the frequency of the packet arrives at the network can be identified, if the arrival rate exists the limitvalue, then there is a chance of DDoS because a huge number of packets are floodedinto the system. Moreover, these packets are dropped.

(4) Analyzing Data Rate:

Next, the data rate is verified with the threshold data rate which is foundby using the private network.

(5) Bandwidth Utilization Analysis:

If the data rate is higher than threshold data,rate the packet is discarded because it may lead to huge utilization of bandwidth which may make the link/network to be jammed. Hence these type of attacks may be prevented.

(6) Updating Threshold:

Since we are using the threshold value which is generated by using the private network, the whole system depends on it, hence for efficient performance the threshold should frequently be updated.

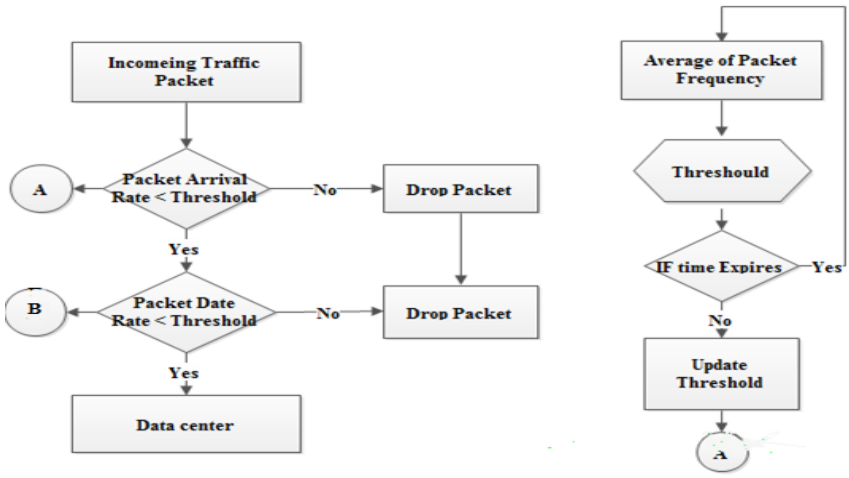

Figure 2: Architecture.

4. Conclusion

Though may require efficient algorithms, systems designs, approaches are made to defend DDoS attack each work well efficiently. Since DDoS attacks are more dangerous, it should be detected and resolved quickly. Our approach defines the way in which the DDoS attack can detect and defend and further refinement may provide an efficient approach to defending and detect DDoS attacks.

References

1. Raj E.D, Babu L.D, Ariwa E, Nirmala M, Krishna,P.V.Forecasting the Trends in Cloud Computing and its Impact on Future IT Business. Green Technology Applications for Enterprise and Academic Innovation; 2014. p.14.
2. Jensen M, Schwenk J, Gruschka N, Iacono LL. On technical security issues in cloud computing. In2009 IEEE International Conference on Cloud Computing. 2009: Sep 21 pp. 109-116.
3. Gellman R. Privacy in the clouds: risks to privacy and confidentiality from cloud computing. InProceedings of the World privacy forum, 2012 Aug 15.
4. Lua R, Yow KC. Mitigating ddos attacks with transparent and intelligent fast-flux swarm network. IEEE Network. 2011 Jul;25(4):28-33.
5. Feng Y, Guo R, Wang D, Zhang B. Research on the active DDoS filtering algorithm based on IP flow. In2009 Fifth International Conference on Natural Computation 2009 Aug 14: Vol. 4, pp. 628-632.

6. Lu L, Chan MC, Chang EC. A general model of probabilistic packet marking for ip traceback. InProceedings of the 2008 ACM symposium on Information, computer and communications security 2008 Mar 18: p. 179-188.
7. Liu H. A new form of DOS attack in a cloud and its avoidance mechanism. InProceedings of the 2010 ACM workshop on Cloud computing security workshop 2010 Oct 8: p. 65-76.
8. Babu L. D, & Krishna P. V. An execution environment oriented approach for scheduling dependent tasks of cloud computing workflows. International Journal of Cloud Computing. 2014; 3(2): 209-224.
9. Krishna, P. V. Honey bee behavior inspired load balancing of tasks in cloud computing environments. Applied Soft Computing.2013;13(5): 2292-2303.
10. Dhinesh Babu L. D, Gunasekaran A, Krishna, P. V. A decision-based pre-emptive fair scheduling strategy to process cloud computing work-flows for sustainable enterprise management. International Journal of Business Information Systems. 2014; 16(4): 409-430.