International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Survey on DDoS Attack in Cloud Network

Monalisa Shinde[1], Shripadrao Biradar[2]

[1]RMD Sinhgad School of Engineering, Pune University, Pune, India

[2]Professor, RMD Sinhgad School of Engineering, Pune University, Pune, India

Abstract: ***Cloud is now a major computing platform. Consequently a question arises about its security. One major type of attack is, a denial-of-service (DDoS) or distributed denial-of-service (DDoS). This attack attempts to make a machine or network resource unavailable to its intended users like bandwidth of network, data structures, operating system and computing power. So we can overcome DDoS attacks in a cloud environment. Here is a survey which provides a depth study on this attack. After the analysis of various scenarios of DDoS attack and cloud environment, we can say that DDoS attack can be minimize. But some strong techniques should be implemented which are suggested in solutions.***

Keywords: Cloud Computing, DDoS Attack, Intrusion Prevention System, Dynamic Resource Allocation, DNS.

1. Introduction

This survey has aim of providing a update on the current cloud environment and DDoS attack scenario. There are various types of types this DDoS attack. There are mainly two categories of DDoS attack. Infrastructure and application layer attacks.

A cloud is made available in a pay-as-you-go manner to public. It has its own some advantages and limitations. This paper also takes a view on it. And some current cloud base system tries to avoid and minimize this DDoS attack with various techniques. So it shows how these mechanisms use advantages of cloud environment. Finally have a conclusion on this all scenario.

2. Cloud Computing

Almost every IT industry needs a big computing infrastructure and services which is of high cost. Cloud computing has potential to provide all this in low cost. It helps to provide this suitable IT architecture and it becomes accessible by using internet.

Cloud computing is one type of computing in which large groups of remote servers are connected together by a network which allows mainly the centralized data storage, and online access to computer resources and services. It increases the various capabilities and capacity of the new software and also of existing software.

Cloud computing make use of networks of groups of servers mainly running consumer PC technology which are of minimum cost. And it also uses specialized connections which spreads data-processing chores across them. They use virtualization techniques.

Cloud Computing is used to refer both the applications delivered which act as services over Internet and systems software and hardware in data centers which provide those services. These services have been called as Software as a Service (SaaS).

A cloud is made available in a pay-as-you-go manner to public, it's called Public Cloud and service which it delivers is called Utility Computing. Some examples of public Utility Computing include Microsoft Azure, Google AppEngine and Amazon Web Services these are some examples of it. The internal data centers of organization or a kind of business which are not available are called as Private Cloud.

Thus Cloud Computing is can be viewed as the sum of Utility Computing and SaaS. But generally, Private Clouds are not included in it.

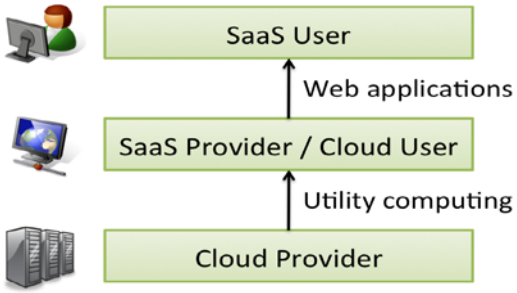

Figure 1: Relationship between Providers and users of Cloud Computing.

Above figure elaborates the relationship between users of cloud and providers of Cloud. Here cloud providers and SaaS providers or cloud users are focused. There is a recursive top level and in that SaaS providers can also act as a SaaS users. For example, a provider of mash up of rental maps might be a user of Craigslist and also of Google maps services.

3. DDoS Attack

There are seven layers of Open Systems Interconnection (OSI) model. Each logical layer has its unique own security. The current trend of Distributed Denial of Service (DDoS) attack basically has two types: Infrastructure DDoS attack (Layer 3 & 4) and Application DDoS attacks (Layer 7).

First type of attack is infrastructure attack. This tries to attack the bandwidth capacity of system. This attack sends very

large number of requests which consumes major part of available bandwidth.

Among these the second type of attack i.e. application attacks, tries to attack on a specific application. It tries to degrade the performance of that application in such a way that finally remote server crashes.

3.1 Infrastructure (Layer 3 and 4)

3.1.1 TCP Synchronization Flooding Attack

To open a TCP connection has 3-way handshaking mechanism is used. When the client begins and sends a SYN message to the server system. Server gives acknowledgement with a message SYN-ACK. And finally connection establishment phase ends with ACK message of client to server. But in this type of attack, attacker don't send ACK message by to the server. So server waits for this acknowledgement message and as it didn't received it resends SYN-ACK message to client. So server gets busy in continuously sending this acknowledgement message and its entire backlog gets filled. Because of this various new connection requests are denied.

3.1.2 Domain Name Server (DNS) Amplification / Reflection Attacks:

This type of attack is also a distributed denial of service (DDoS) attack. By spoofing the victims address, an attacker tries to send request message of DNS lookup. It sends this request to an open DNS resolver. Then DNS server also sends the response to the source address which was in spoofed message. And response is considerably bigger than request. So attacker can maximize the traffic to victim. And attacker can majorly attack the victim's system with just a little effort.

3.1.3 UDP Flooding Attack:

A User Datagram Protocol (UDP) UDP flood is also one type of attack where bandwidth is being targeted. In UDP session establishment of client and server is not required, i.e. states are not required. The victim generates large amount of UDP packets at various ports. Then victim system determines any waiting application on the destination port.

At the time when system gives response to various incoming packets it responds by using an IMCP unreachable message if no one application is waiting at the destination port. So the victim system gets attacked by the overloading of many UDP responders.

3.1.4 ICMP Flooding Attack

The Internet Control Message Protocol (ICMP) flood, is also an DoS attack. It is a ping based type of attack. Very large numbers of packets of ICMP are sent to a server. This attempt to fell down the TCP/IP stack of the server which causes delayed responses to the coming TCP/IP requests.

3.2 General Application-Layer DDoS Attack Categories

3.2.1 Request Flooding Attack

Request-Flooding Attacks can occur at the time when the requests of large size are sent continuously to the server. Like, DNS queries, HTTP GETs, SIP INVITEs, etc.

3.2.2 Asymmetric Attack

Asymmetric Attacks can also occur if requests which consume big amounts of server resources come continuously. Request like consumption of disk space, memory and CPU, etc. It decreases the performance of the server severely.

3.2.3 Repeated One-Shot Attack

Repeated One-Shot Attacks occurs with TCP session. Attacker sends request of very large workload across many sessions of TCP. By this server services greatly degrade.

3.2.4 Application Exploit Attack

Application Exploit Attacks occurs when various applications or operating system of server becomes faulty. Attacker gets the whole control of that application or operating system. Some attacks are of this category like, Scripting problems, Structured Query Language (SQL) injection, manipulation of hidden field, overflow of buffer, etc.

4. Some Current Solution

Generally a cloud possesses profound resources and it has full control on its resources. Also cloud has dynamic allocation capability of its resources. Therefore, cloud offers the potential to mitigate DDoS attacks. But, for individual cloud hosted server DDoS attack is major problem.

Some researchers have proposed mechanisms to counter the DDoS attacks against the They proposed that when a DDoS attack occurs, system employ the idle resources of the cloud. Clone the sufficient intrusion prevention servers immediately filter out attack packets. This guarantees the quality of the service for legitimate users.

To minimize DDoS attack extra reserved resources are allocated. System dynamically allocates resource to targeted customers of individual cloud. Also provide a Intrusion Prevention System (IPS) at various access points which are placed in internet and cloud. All incoming packets will be monitored by this IPS. Whenever a DDoS attack is experienced by system, this mechanism will allocate extra reserved resources. And a resource pool will maintain the track of all reserved resources.

Based on the strength of the packets coming, system clones new virtual machines depending on the different image files of IPS. These all IPS together try to drop attack packets. When DDoS becomes less effective, automatically IPS of system will be dismissed and the virtual machine also dismissed on which the IPS is located which in turn releases the extra resources allocated from pool.

The major issue in this is to allocate extra resources to system, there is issue that how detection algorithms and filtering algorithm works and what's there accuracy is. The most harmful DDoS attack can be minimized by using cloud platform itself. A mechanism called dynamic resource allocation has ability to allocate all the available resources dynamically. So this system uses this mechanism which automatically will coordinate with all the available resources in the cloud. This will minimize the DDoS attacks on customers of individual cloud.

The method will have a model based upon queuing theory. This model will estimate the resource allocation against the strengths of DDoS attack. Also the data set of real world will be analyzed. And these various experiments and analysis will help to prove that DDoS attack really becomes lower by this proposed method.

Cloud support Infrastructure as a Service (IaaS). To support this generally cloud makes use of virtualization of data centers. A data center of a cloud maintains a catalog which stores list of virtual machine images which are available. Images may contain the operating system only. Operating systems like Windows or Linux Red Hat It may contain main applications like database management systems or even be created by users.

Data centers provide VMs which in turn provides various compute resources applications and various services. This system should be well scalable and elastic. But it's very crucial thing to provide virtual machines fast.
One problem is gigabytes order size VM images. To read an image it takes long time and also more time required to transfer images from the network.

Second problem is the use of centralized servers. Cloud uses centralized servers for storing and dispensing VM images. So it becomes bottleneck when clients of large population send bursty requests. It's also found that, a VM image create small number of instances at given time. Here point to point file sharing approach becomes ineffective.

So, a new approach for this is called as chunk-level Virtual machine image Distribution Network (VDN). Many times files of different VM images have much number of common chunks of data. As data centers have hierarchical network topology, it can reduce the VM instance provisioning time.

It can also have advantage of minimum overhead of chunk location information maintenance. And by this VDN achieves fast operations. Nearly, large VM images 30–80x speed up even under heavy traffic.

5. Conclusion

In this paper, it's highlighted that using a cloud-based system is very advantageous. But there are some main problems about its security. Cyber criminals still have a best way of attack i.e DDoS attacks. By this individual cloud environment gets highly affected. But every cloud environment possesses a large set of resources which can mitigate the impact of DDoS attack in considerable amount. So a strategy can be planned to allocate these profound ideal resources to customers when system experience DDoS attack.

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 and M. 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.
[5] 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.
[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, ''Defending Against 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.
[11] S. Chaisiri, B.-S. Lee, and D. Niyato, ''Optimization of Resource Provisioning Cost in Cloud Computing,'' IEEE Trans. Serv. Comput., vol. 5, no. 2, pp. 164-177, Apr./June 2012.
[12] J. Idziorek, M. Tannian, and D. Jacobson, ''Insecurity of Cloud Utility Models,'' IT Prof., vol. 15, no. 2, pp. 22-27, Mar./Apr. 2012.
[13] M.H. Sqalli, F. Al-Haidari, and K. Salah, ''Edos-Shield-a Two- Steps Mitigation Technique against Edos Attacks in Cloud Computing,'' in Proc. UCC, 2011, pp. 49-56.
[14] Q. Wang, K. Ren, and X. Meng, ''When Cloud Meets Ebay: Towards Effective Pricing for Cloud

Computing,'' in Proc. INFOCOM, Mar. 2012, pp. 936-944.
[15] Q. Wang, K. Ren, and X. Meng, ''When Cloud Meets Ebay: Towards Effective Pricing for Cloud Computing,'' in Proc. INFOCOM, Mar. 2012, pp. 936-944.

Author Profile

Monalisa Shinde received the B.E. degree in Computer Engineering from SSVPS's BS Deore College of Engineering, North Maharashtra University in 2009.

Shripadrao Biradar is working as Professor in RMD Sinhgad School of Engineering, Pune University, Pune, India.