A Survey on Methods to Defend against DDoS Attack in Cloud Computing

SARA FARAHMANDIAN, MAZDAK ZAMANI, AHAD AKBARABADI, JOOBIN MOGHIMI ZADEH, SEYED MOSTAFA MIRHOSSEINI, SEPIDEH FARAHMANDIAN
Advanced Informatics School
Universiti Teknologi Malaysia
54100 Kuala Lumpur
MALAYSIA
sarah.farahmandian@gmail.com, mazdak@utm.my, ahad.akbarabadi@gmail.com, joobin_2002@hotmail.com,smmh1987@gmail.com, sepideh_sf7@yahoo.com

Abstract: Cloud computing is a revolution in IT technology by providing a shared pool of virtualizes resources for its users to pay as they use. This technology is based on two crucial concepts as virtualization and abstraction, which increased the ability of on demand access through the available resources in the cloud without any investment in new infrastructure. Security is one of the most challenges for both cloud provider and cloud consumer. In recent years DDoS attack is one of the most serious threats against cloud computing. Since cloud built on the fundamental of distributed environment, it is easier for an intruder to launch a DDoS attack against available resources and services of a cloud computing environment. This paper introduces cloud computing, Virtualization and DDoS attack. A review and comparison of the existing methods against DDoS attack on cloud computing is presented as well.

Key-Words: Cloud computing, virtualization, DDoS attack, threat, intruder, distributed environment

1 Introduction

1.1Cloud computing

Cloud computing was a very old dreaming of computing as a service which would be used for transforming a huge portion of the IT industry, and also updated the usage of software pretty attractive as a service. It even created a great change in design and purchases of hardware and virtual technology in IT world. In recent years, this technology is basically used as a platform for sharing resources such as software, application, Infrastructure resources, and even for business processes[1,2].

Technology of cloud computing is based on using the internet and remote servers for preserving data and applications. Being able to use the application without any installation on personal systems by just accessing to the internet is an interested part in cloud computing. [3,18,19].

The grid computing, distributed computing and parallel computing in Service Oriented Architecture (SOA) is as application operation in cloud computing. This technology could be accessible everywhere just by using any digital devices such as laptops, smart phones, cell phones, which are capable of connecting to the internet and cloud base services such as social networking, webmail and video viewing. It also allows well-organized by following centralized storage, memory, process-sing and bandwidth [4,17,18].

The system layer (is a virtual machine concept of a server), the platform layer (a Virtualization operating system of a server), and application layer (which include web applications) are three fundamental layers in cloud computing. Three services model which is involved in cloud computing are named as Platform as a Service (PaaS), Infrastructure as a Service (IaaS), and Software as a Service (SaaS)[5,17,20].

SaaS gives ability to users for working with their software far from any anxiety of installing and running their applications on their own systems[5].

The PaaS layer provides a platform for users whom their application can be run like Java's platform. Actually, PaaS makes customer able to utilize of the provider's cloud infrastructure for deploying their web applications and other software by using supported vender's programming languages. IaaS provides a large Infrastructure, managing networks and maintaining user's information in a protected way. In IaaS, providers by using virtualization software share their hardware among multiple customers, which refer as "multiple tenants[5,21,22].

1.2 Virtualization

In cloud computing one of the critical parts is virtualization, which plays a significant role in constructing efficient and flexible usable of hardware devices. Actually, an abstraction of computer resources was named as Virtualization. In recent years, Virtualization is used in majority level such as networks, and system storage, CPU, memory, application stacks and databases, which are also useful for improving security of systems, availability, reliability, and especially in terms of reducing costs and present a superior flexible system[6,22,26].

By simulating the hardware, virtualization gave permission to multiple virtual machines to run a different operating system and application on single computers, which achieve multi tenancy and high scalability[7,23].

Virtual machines have permission for sharing the resources of host machine but in a way, which can be able to provide isolation between the virtual machines and the host[7,24].

In the virtualization world when a client utilizes a system, dealing directly with a view which is present in the operating system with an abstraction of all the available physical elements. With Inspiration of this logical view description of what virtualization technology tries to do is more understandable, which is building a few different logical views from a physical machine which would be used by several users at the same time. [8].

1.3 DDoS attacks

Although using virtualization brings more benefits in cloud computing technology, there are critical security issues, which should be concerned in cloud computing such as Denial-of Service (DoS) and Distributed Denial-of Service (DDoS) attack, which can demolish the availability of cloud networks by attacking to virtual servers and resources.

The biggest purpose of an attack such as DoSand DDoSis to make network resources such as servers, and storage inaccessible for all intended clients. In the majority of cases of DoS attacks, the attacker usually targets sites or services, which are on high-profile web servers such as banks, credit card payment gateways and even in some cases Domain Name Servers,but it is not just restricted to this field. It even used to attack on CPU, Storages, and the other resources on Networks[9].

One of the most jeopardy threat for service availability of cloud computing is DDoS. DDoS attacks actually are same as DoS attacks but in a way which a massive amount of hosts in the network executes DoS attacks via a synchronized behavior to one or more targets. These kinds of attacks enormously increased based on bandwidth and technique[10,25,27].

In cloud, DDoS attacks harshly decreased the performance of cloud services. One of the usage of DDoS attacks for the attacker is that make them able to freely control information through the networks and even by creating specific information on specific time decided that which information can be accessible for clients and which one not[11].

2 Defense Methods against DDoS attack

To defend against DDoS attack in cloud computing there are several mechanisms which are discussed in the following section.

2.1 CTB Model to defend against DDoS attacks

One method is using of Cloud Trace Back (CTB) and Cloud protector. CTB would be utilized in both LAN and Grid network structure. The purpose of having CTB in our cloud network is to have ability to trace back the source of these attacks and also make use of a neutral network named cloud protector is to detect and filter such attack traffic[12].

CTB and Cloud Protector are located between the each cloud web service to defense against XML-based DDOS attack. This method gave ability to cloud networks for detecting and filtering most of the attack's bases on DDoS. Fig. 1 shows the CTB place in the cloud environment[12].

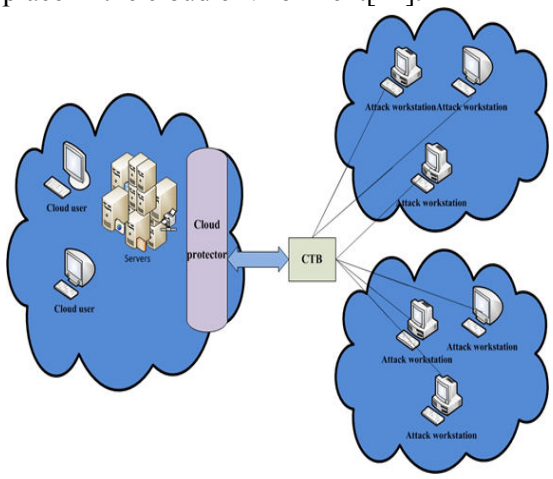

Fig. 1 CTB and Cloud Protector

2.2 Defend Against Denial of Service Attack with VMM

By getting the advantages of virtual machine monitor (VMM) to monitor virtual machine resource availability proposed a technique for mitigating operating system and tagged application lively into the isolated environment. Inside the VMM there are three components named as a tagger, duplicator, and a detector. Fig. 2 showed the design of the proposed model and its component relationship.

The aim of this method is that monitors and computes the available amount of current system resources and compares it with a given value as threshold to find the existence of an attack. After detecting an attack this method lively transforms the OS and specific applications into an isolated place which also is a virtual machine. The advantages of this method is that without stopping OS performing makes the system able to escape from this kind of attack[13].

2.3 Distributed Cloud Intrusion Detection Model

Using Intrusion Detection System in Virtual Machine for securing cloud networks against DDoS attacks is another method for solving this problem. IDS located on the virtual switch and gave ability to system to log the network traffic inbound and out-bound through the database for auditing. Intrusion detection system examined all packets to find a type of attack base on predefined rules. Virtual server by getting the help of IDS could be able to recognize the security risks involved in such attacks[11].

Using this method to defend against DDoS attack in the cloud could be fed away most of the problem. To have an effective IDS with ability of working in the cloud the proposed model is based on a Distributed cloud IDS which uses of multi-threading method for enhancing IDS performance over the cloud infrastructure.

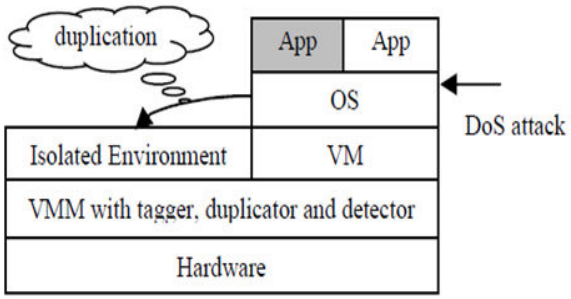

Fig. 2 Proposed model by using VMM

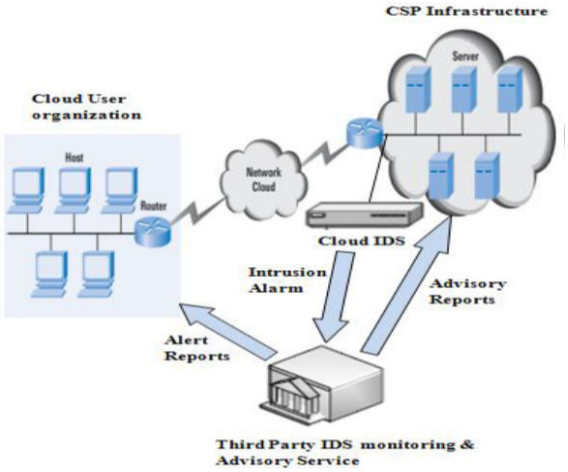

Fig. 3 DIDS in cloud computing

Actually, it is a Network Intrusion Detection (NIDS), which can sensitize and monitors network traffic in addition to testing for malicious packet. Intrusion alarms are sent to a third party monitoring service which offer a report to cloud user organization management system and a consultative report to the cloud service provider. Model showed in Fig. 3 which explained the process of the DIDS[11].

2.4 Endpoint Mitigation of DDoS Attacks Based on Dynamic Threshold

This method is based on determining a dynamic threshold. It concentrates on deploying a SecureNIC and also observing the server load to find any abnormal activity to defend against DDoS attack. The Fig. 4 illustrated a general view of this method by usage of SecureNIC[14].

All incoming packets with their own IP address monitored through this SecureNIC to find any match attack traffic pattern. When it finds any match traffic then discards the next packet of that particular IP address[14].

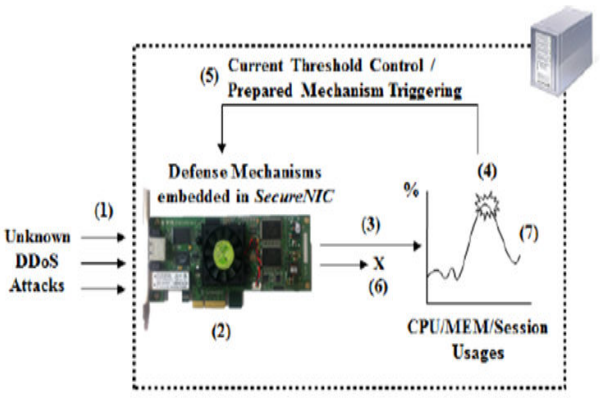

Fig. 4 SecureNIC Overview

2.5 Optimal Control of DDoS defense with Multi- Resource Max-Min Fairness

Defense mechanisms named FFDRF (Feedback Filtering with Dual-Resource fairness) was proposed against DDoS flood attacks by using control theory which was installed filters on the edge of routers. This method is more effective in terms of CPU consuming flood attack. The most attention of this proposed model was based on resource allocation problem. It modified a threshold between routers and the victims by using feedback[15]. This proposed model was attention as a resource allocation problem which considered both processor time and bandwidth as a two important factors. To be effective against this attack only need to implement on the edge of routers.

2.6 A Filter Tree Approach to Protect Cloud Computing against XML DDoS and HTTP DDoS Attack

A Filter Tree approach was proposed to protect cloud against HTTP-DDoS and XML-DDoS attacks. They present a cloud defender with three steps between client and service provider and tried to stop attacking before catch the cloud. This method use IP addressed to recognize and trace back the illegitimate VMs. Cloud defender is included five steps such as sensor filtering, Hop counts filtering, IP Frequency Divergence Filter, Confirm legitimate user IP Filter, and Double Signature Filter. Fig. 5 showed the proposed model. [16].

2.7 Confidence-Based Filtering (CBF) method Analysis

Chen et al. (2011) deployed this method base on non-attack period and attack period. In non-attack period time lots of legitimate packets are captured and analyzed for creating a normal profile according attribute pairs inside the TCP and IP header. Two amounts are computed in CBF which are Confidence and CBF score. Confidence actually is frequency of single and pair attribute in the packet. This method included discarding threshold which always compared with a CBF score for using at the attack period time. Because it is not based on attack severity the performance of this method is better than PacketScore.

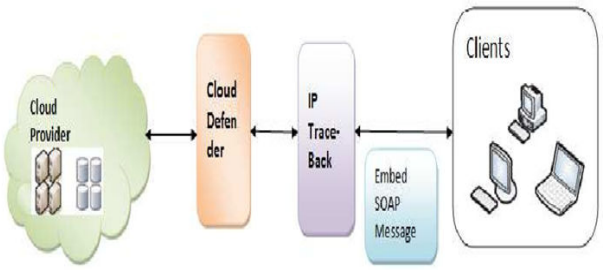

Fig. 5 Filter Tree approach

The performance of CBF in depended to the attack situation for example in general and mix attack type its performance is higher but in attacks such as SQL slammer worms is lower. CBF worked efficiently in large amount of traffic.

2.8 Protecting Cloud Web Services from HX-DoS attacks using Decision Theory

One of the major threats that cloud provider struggle with is based on HX-DoS attack or HX-DDoS attack. This kind of attack tried to demolish the cloud provider's communication channel. So to defend against this kind of attack this method proposed a new defense system named as Pre-Decision, Advance Decision, and Learning System (ENDER). To be able to distinguish between illegitimate and legitimate packets, this method used two decision theories. This method also used Reconstruct and Drop (RAD) to filter disruptive message before coming to the victim target[12]. Fig. 6 shows the overview of this proposed method.

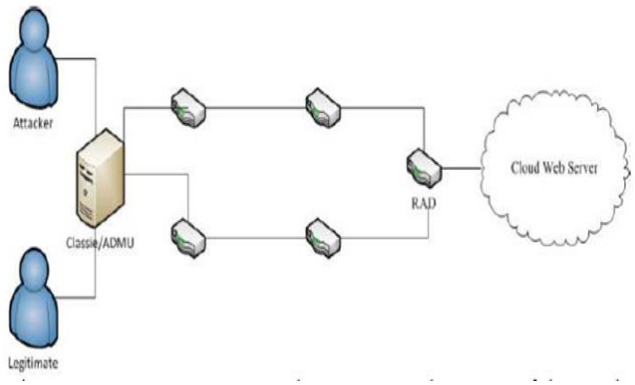

Fig. 6 Overview of ENDER

3 Conclusion

Table 1 indicates a summary of mentioned defense methods against DDoS attack on cloud computing. Cloud computing brings numerous benefits into the IT technology. In spite of being useful, there are several challenges keys in termsof this kind of networks security management is most important. By using cloud through the organization, attacker move their interest to this area and because characteristic of cloud it is easy for them to impact the huge disaster into the whole network. So, working in this area is so important for internet future.

Virtualization is fundamental of cloud computing. Virtualization gives the ability of running several different OS into the only one Host system. Every user has its own VM and do not access to the other VMs. For security, virtualization also brings several challenges and vulnerability into the networks which are so dangerous in this kind of network such as VM to VM attack, Hypervisor attack, and also one of the famous attacks called DDoS attack. To badly impact on availability of network services on cloud environment, DDoS attack is a famous one. There are several kinds of DDoS attack which can simply turn off the services into the network. Several methods have been defined especially for preventing, detecting, and reacting against this kind of attack.

References:

[1] Armbrust, M., et al., A view of cloud computing. Communications of the ACM, 2010.

[2] Zhang, L.J. and Q. Zhou. Cloud computing open architecture. Web Services, 2009.

[3] Jain, P., D. Rane, and S. Patidar. A survey and analysis of cloud model-based security for computing secure cloud bursting and aggregation in renal environment. Information and Communication Technologies (WICT), 2011 World Congress on. 2011. IEEE.

[4] Bakshi, A. and B. Yogesh. Securing cloud from ddos attacks using intrusion detection system in virtual machine. Communication Software and Networks, 2010. ICCSN'10. Second International Conference on. 2010. IEEE.

[5] Roschke, S., F. Cheng, and C. Meinel. Intrusion detection in the cloud. In Dependable, Autonomic and Secure Computing, 2009.

[6] Xing, Y. and Y. Zhan, Virtualization and Cloud Computing. Future Wireless Networks and Information Systems, 2012: p. 305-312.

[7] Sabahi, F. Virtualization-level security in cloud computing. In Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference on. 2011. IEEE.

[8] Dong, H., et al. Formal Discussion on Relationship between Virtualization and Cloud Computing. In Parallel and Distributed Computing, Applications and Technologies (PDCAT), 2010 International Conference on.

[9] Cha, B. and J. Kim. Study of Multistage Anomaly Detection for Secured Cloud Computing Resources in Future Internet. In Dependable, Autonomic and Secure Computing.

[10] Li, M. and M. Li, An adaptive approach for defending against DDoS attacks. Mathematical Problems in Engineering, 2010. 2010.

[11] Gul, I. and M. Hussain, Distributed Cloud Intrusion Detection Model. International Journal of Advanced Science and Technology, 2011.

[12] Chonka, A. and Y. Xiang, Protecting Cloud Web Services from HX-DoS attacks using Decision Theory. 2012.

[13] Zhao, S., K. Chen, and W. Zheng. Defend Against Denial of Service Attack with VMM. In Grid and Cooperative Computing, 2009. GCC'09. Eighth International Conference on.

[14] Kim, D., et al., Endpoint Mitigation of DDoS Attacks Based on Dynamic Thresholding. Information and Communications Security, 2012: p. 381-391.

[15] Wei, W., Y. Dong, and D. Lu. Optimal control of DDoS defense with multi-resource max-min fairness. in Cybernetics and Intelligent Systems, 2008 IEEE Conference on

[16] Karnwal, T., S. Thandapanii, and A. Gnanasekaran, A Filter Tree Approach to Protect Cloud Computing against XML DDoS and HTTP DDoS Attack. Intelligent Informatics

[17] Zeidanloo, H. R., BtManaf, A., Vahdani, P., Tabatabaei, F., and Zamani, M. (2010). Botnet detection based on traffic monitoring. Paper presented at the Networking and Information Technology (ICNIT)

[18] Shohreh, H., Mazdak, Z., and Roza, H. (2012). Dynamic Monitoring in Ad Hoc Network. Applied Mechanics and Materials.

[19] MaziarJanbeglou, Mazdak Zamani, Suhaimi Ibrahim. Improving the Security of Protected Wireless Internet Access from Insider Attacks. Advances in information Sciences and Service Sciences (AISS). July 2012.

[20] MojtabaAlizadeh, Mazdak Zamani, Ali RafieiShahemabadi, JafarShayan, Ahmad Azarnik. A Survey on Attacks in RFID Networks. Open International Journal of Informatics (OIJI). Vol 1 (2012).

[21] MojtabaAlizadeh, Wan Haslina Hassan, MazleenaSalleh, Mazdak Zamani, Eghbal Ghazi Zadeh. Implementation and Evaluation of Lightweight Encryption Algorithms Suitable for RFID. Journal of Next Generation Information Technology.

[22] Zeidanloo, H. R, Abdul Manaf, A., VahdaniAmoli, P., Tabatabaei, F., and Zamani, M. "Botnet Detection Based on Traffic Monitoring". IEEE, International Conference on Networking and Information Technology, Manila, Philippines, Jun 2010.

[23] HosseinRouhaniZeidanloo, Mohammad JorjorZadehshooshtari, PayamVahdaniAmoli, M. Safari and Mazdak Zamani, "A Taxonomy of Botnet Detection Techniques".International Conference on the 3nd IEEE International Conference on Computer Science and Information Technology. China, 2010.

[24] MaziarJanbeglou, Mazdak Zamani, and Suhaimi Ibrahim. Redirecting Network Traffic toward a Fake DNS Server on a LAN. 3rd IEEE International Conference on Computer Science and Information Technology. July, 2010. China.

[25] Beigzadeh, S., Mazdak Zamani, Suhaimi Ibrahim, and Maslin Masrom. Design and Implementation of a Web-Based Database-Centric Management Information System for a Social Community. International Conference on Information Systems and Computational Intelligence (ICISCI 2011).

[26] EghbalGhazizadeh, Mazdak Zamani, Jamalul-LailAbManan and AbolghasemPashang. A Survey on Security Issues of Federated Identity in the Cloud Computing. The 4th IEEE International Conference on Cloud Computing Technology and Science (CloudCom 2011). Dec 2012. Taipei, Taiwan.

[27] Maryam Gharooni, Mazdak Zamani, and Mehdi Mansourizadeh. A Confidential RFID Model to Prevent Unauthorized Access. 3rd International Conference on Information Science and Engineering .China, 2011.

TABLE 1 A SUMMARY OF DEFENSE METHODS

Year	Title	Focus	Scalability	Method	Propose
2011	CBF:A Packet Filtering Method for DDoS Attack Defence in Cloud	DDoS attack	Yes	Packet Filtering	A packet Filtering method based on scoring the packets during the attack period
2012	Protecting Cloud Web Services from HX-DoS attacks byDecision Theory	HTTP/ XML-DoS	Yes	Decision Methods	Proposed a Defence method named ENDER
2010	CTB Model to defend against DDoS attacks	XML-based DDOS	Yes	Traceback Method	A Traceback methods to defend against DDoS attack
2009	Defend Against Denial of Service Attack with VMM	DoS attack	No	Resource Monitoring	To mitigate OS and particular application in isolated location during the attack detection
2012	A Filter Tree Approach to Protect Cloud Computing against XML/HTTP DDoS Attack	XML- DDoS and HTTP DDoS attacks	Yes	Filtering Method	A model against DDoS attack based on combination of several detection methods.
2011	Distributed Cloud Intrusion Detection Model	DDoS attack and cross site scripting	Yes	IDS Method	A Distributed IDS model by using a third party as an alarm sender through both cloud provider and customer
2012	Endpoint Mitigation of DDoS Attacks Based on Dynamic Threshold	DDoS attack	No	Traffic Monitoring	Create a SecureNIC based on dynamic traffic monitoring comes from each IP address
2008	Optimal Control of DDoS defence with Multi-Resource Max-min Fairness	CPU-consuming Flood	No	Resource monitoring	Filtering in edge of routers and using a threshold filter

ISBN: 978-1-61804-162-3