Indian Journal of Science and Technology Vol. 5 No. 6 (June 2012) ISSN: 0974- 6846

Availability challenge of cloud system under DDOS attack

Aboosaleh Mohammad Sharifi*[1], Saeed K. Amirgholipour[1], Mehdi Alirezanejad[2], Baharak Shakeri Aski[1] and Mohammad Ghiami

[1]*Department of Computer, Ramsar Branch, Islamic Azad University, Ramsar, Iran*

[2]*Department of Computer, Firuzkooh Branch, Islamic Azad University, Firuzkooh, Iran*

sharifi@iauramsar.ac.ir*

Abstract

Cloud computing is a distributed architecture that has shared resources, software, and information is provided to computers and other devices on a scalable platform and demand. Availability of the cloud services is one of the key security issues in it. Distributed Denial of Service (DDoS) is an attack that threats the availability of the cloud services. In this paper, effect of the DDoS attack on the cloud is investigated. Therefore, a model for attack based on the DDoS is designed, and then we simulate a cloud system on the experimental environment. Experiments show that the cloud system is vulnerable to this attack. In order to confronting this attack, several solutions are proposed in this paper. We suggest load balancing and honeypots beside the intrusion detection systems (IDS) is used to defend from the attack.

Keywords. Cloud, DDoS Attack, IDS, Honeypot, Load Balancing.

Introduction

Today, cloud computing is one of the most efficient ways of using resources. Cloud has no specific location, and it is unclear how much size it has. Only, we know what services the cloud offers to us. When using of the cloud computing is going to common, no longer need to pay money for software and hardware, instead of that, how much we use a service is our cost (Weiss, 2007).

Cloud systems give many services to customers. Such as software which is hosted in the cloud, networks as a Service (SaaS), examples of SaaS are Google Docs, MS Office Live (Vidyanand Choudhary, 2007). The cloud provides web space to users for storing their data, Data as a Service (DaaS), for example, Dropbox (Bhaskar Prasad Rimal *et al*., 2009). Providing a platform for customers to develop applications and services that run under the cloud system, Platform as a Service (PaaS), such as Google AppEngine (Ian Foster *et al*., 2008). Finally, the cloud provides the scalable computing power which is deriving a benefit of the cloud, Infrstructure as a Service (IaaS), such Amazon EC2 (Luis *et al.,* 2011).

First, to take advantage of cloud services, connection between the user and the server cloud must be estalished. After confirming the identity of users, the service provider must supply requested services. Despite the many benefits of cloud computing, users still do not have full trust for the cloud services and do not put their sensitive information in the cloud (Amardeep Singh & Monika Verma, 2011).

There are several challenges for customers to have no trust to the cloud computing. Security, performance and availability are important issues of cloud computing. Security is a key issue in the cloud systems, which afects on developing for it. A group of people might not accept that their personal information is on the cloud or their applications to run on the supercomputer resources, because of a possibility of abuse information by other users. The next challenge is performance, how to use resources to solve complex problems. However, there are problems in the cloud systems; first, cloud is not fully known yet, secondly, there is continuous variability of rsources. Therefore, it might not be completely optimized use of system capabilities to the cloud. Last, the availbility of services and resources in the cloud is another challenge. The availability is the customer uses the cloud services at any time and in anywhere (Mihai Christodorescu *et al*., 2009).

The challenge of availability of the cloud system can be referred to Distributed Denial of Service (DDoS) attacks. DDoS can be described as adesign attack for disabling normal service in the network. When, this attack happened, the access to a network server or resource is blocked for legal costumer. Imagine that whereas a customer tries to access a cloud system for using it, face with the message of “this page cannot be displayed”, this message and unavailability of customers take not only minutes even for hours and days long. This state might be a result of DDoS attacks (Jose Nazario, 2008).

In this work, the effect of DDoS attack on availability of the cloud system is studied. First, we proposed a scenario for DDoS attack based on flood to run on the cloud system with different features. Next, this attack performs on the cloud. Last, the obtained results are analyzed to extract solution to prevent this type of attack.

Cloud computing

The data center is home to the computational power, storage, and applications necessary to support an eterprise business. Fig. 1 shows a typical data center structure. The data center is a part of the network of enteprise business. The data center infrastructure is central to the IT architecture, from which all content is sourced or passes through. Proper planning of the data

Indian Journal of Science and Technology Vol. 5 No. 6 (June 2012) ISSN: 0974- 6846

Fig. 1. Typical model of data center

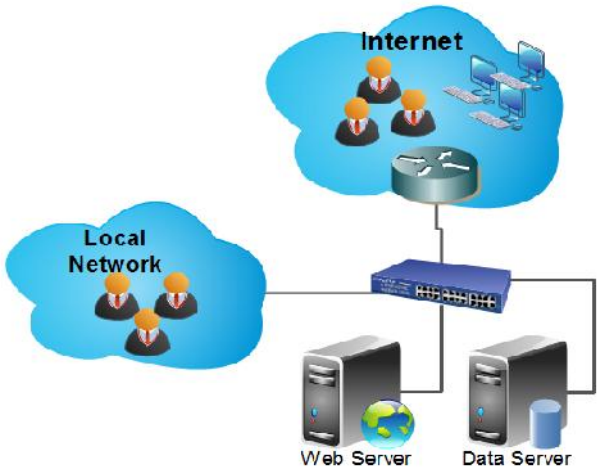


Fig. 2. The cloud computing model

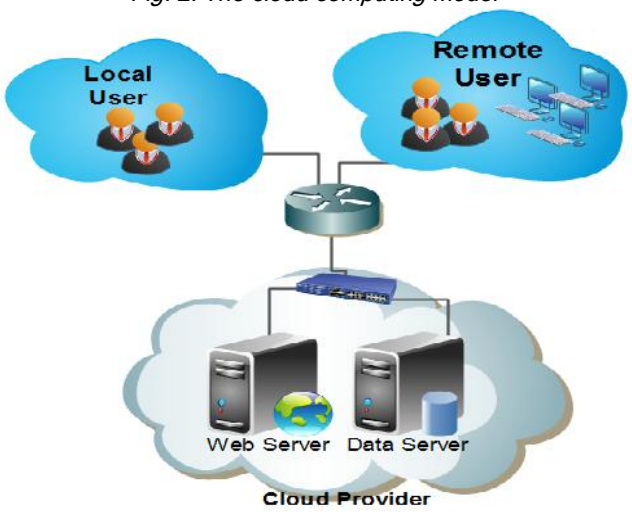
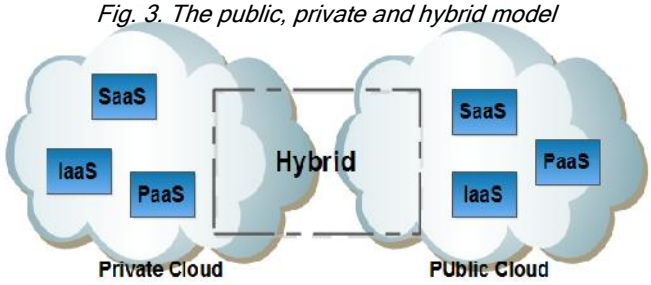


Fig. 3. The public, private and hybrid model



center infrastructure design is critical, and performance, resiliency, and scalability need to be carefully considered.

Consider a business with several enterprises' branches in separate place in a country or the world, then for doing work in each branch; we need to construct the equal data center for each enterprise. Construction of this busness in this way is expensive. Cloud is a suitable solution for this problem. Thus, data center segment (application and data) is located as a host in the internet. Then legal users can be connected to the cloud with a simple internet connection. Fig. 2 shows the cloud computing model.

Cloud computing has several advantages over similar technologies. Cloud is more remote Accessible. With cloud computing, your business is not limited to a particular location. You can access the services from anwhere. Easy expansion is another feature of cloud. You can quickly access more resources if you need to expand your business. You need not buy more infrastructures. You just need to inform your cloud provider about your rquirements, and they will allocate resources to you.

The same approach is done if you request to use fewer rsources. Resource sharing is one of the key features of the cloud. In cloud computing, resources are shared at the network, host and application level. All resources including expensive networking equipment, servers, IT pesonnel, are shared, therefor the cloud have a lower cost. Management of data and application are faster than the traditional data center. This is closely aligned with cost savings. Since cloud has very low upfront costs, the maagement approval process is greatly accelerated, causing faster innovation. In fact, costs are so low, that indviduals can easily fund the expense personally to demonstrate the benefits of their solution, while avoiding organiztional inertia (Catteddu & Hogben, 2009).

Cloud deployment models

Public cloud

The most common model of cloud is public. The application and services (SaaS, IaaS, DaaS and PaaS) are available to customer in public cloud. Each customer can use this service and application by registering and acessing to the cloud. Each user pays for the usage of those services. In this cloud, cloud providers are hosted of multiple data center. Multiple users can access to cloud at the same time and get their favorite's services (Victor Chang *et al.*, 2010).

Public cloud

Private cloud is mixed of the cloud computing on a private network. They allow users to have the profits of cloud lacking of some of the drawbacks. Private clouds grant complete control over how data is managed and what security measures are in place. This can lead to users having more confidence and control. The major issue with this model is that the users might spend large costs to buy the infrastructure for implementation of the cloud and also have to manage the cloud themselves (Victor Chang *et al.*, 2010).

Private cloud

Private cloud is mixed of the cloud computing on a private network. They allow users to have the profits of cloud lacking of some of the drawbacks. Private clouds grant complete control over how data is managed and what security measures are in place. This can lead to users having more confidence and control. The major issue with this model is that the users might spend large costs to buy the infrastructure for implementation of the

Indian Journal of Science and Technology Vol. 5 No. 6 (June 2012) ISSN: 0974- 6846

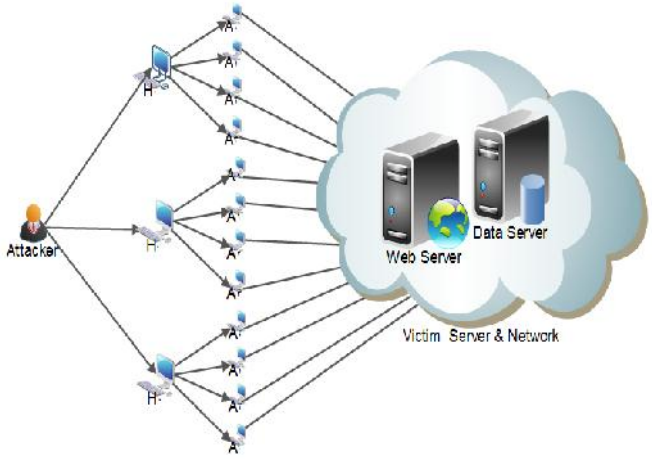
cloud and also have to manage the cloud themselves (Victor Chang *et al*., 2010).

Hybrid Cloud

Many believe that for cost optimization in an organization, a balance between public and private clouds is needed. Hybrid Cloud allows the organizations to get advantage of both deployment models. For example, an organization could hold sensitive information on their private cloud and use the public cloud for handling large traffic and demanding situations. However, since this hybrid cloud solution is commonly bound together by prprietary technology, it will only be embraced by enterprise computing in the future as standards are developed (Victor Chang *et al.,* 2010). Fig, 3 shows the public, private and hybrid cloud model.

DDoS

Fig. 4. The DDoS attack model



The availability of the services means customers expect services available to them after a reasonable amount of time. Availability of the services might be violated either by different methods such as system errors, hardware and software constraints, and malicious attacks from outside. Imagine that the customer is trying to use the cloud services; the message such as “no access to services” will appear and this message is not for a few seconds or minutes, but hours and days to take. This status might be as a result of denial of service (DoS) atacks (Basheer & Manimaran, 2009).

The DoS might be described as an attack designed to disable server services in a network. The attack comes a time when access to a computer user is blocked. This could be the result of a malicious act by the other user. DDoS means that many systems are deadly agree to each other to launch an attack against the victim's system, which results in disruption of service for legitimate users. DDoS can be resulted of each intentional or unintentional attack. If a computer hardware, software and data are not available, productivity can be lost, even if nothing did not damage. Attackers acquire their agents to attack via Internet with infect and control vulnerable hosts and then their data packets are sent at no cost to the victim using the network (Christos Douligeris & Aikaterini Mitrokotsa, 2003).

The most common process of DDoS attacks has these stages. First, computers in the network scan with uing tools such as the port scanner by the attacker. Port Scanning software is one of the most popular investigation technique's attackers use to discover services they can intrude. All computers connected to a Local Area Network (LAN) or the internet runs many services that listen at well-known and not so well known ports. A port scan helps the attacker find which ports are accessible. Principally, a port scan consists of sending a message to each port, one at a time. The kind of response received indicates whether the port is used and can therefore be probed futher for weakness. In the next stage, attackers try to intrude to the vulnerable hosts, and install wrecking script on them. Vulnerable hosts are divided to the handlers and agents. Handlers are intermediate interfaces for tranform command of the attacker to the agents. Agents are a performer of attack, which is designed by the main attacker. Architecture of DDoS attack is shown in the Fig. 4.

Attack

Here, a scenario has been proposed for performance evaluating of the cloud system under the DDoS attacks. In this scenario, the cloud system with a DDoS attack and intrusion detection systems (IDS) is investgated (Asayuki Murakami & Nakaji Honda, 2007). The IDS is reacting to the attacks. We consider the cloud is the data-storage system (DaaS). In this work, we have tried to increase the accuracy of the results by implmenting a clever DDoS attack on the cloud system, in order to the IDS could not detect an attack easily. In this attack, the attacker sends flood packets to the cloud system in specified time intervals in the intermittent manner with low period time while the cloud is down. In the figure 4, attack, model is shown.

In this figure, we have three handler nodes (H0, H1, and H2) and each handler node has four agents (Ai, 0, Ai, 1, Ai, 2, Ai, 3). In each agent, there is software to implement DDoS attack. Command of Attacker sends to their handlers for attack by their agents.

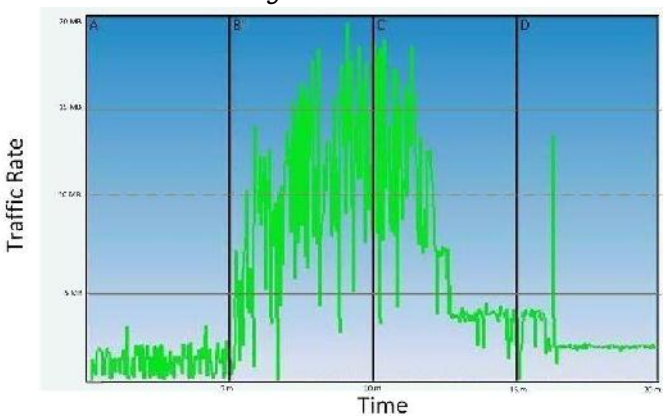
Model of attack

IDS designed based on the behavioral threshold. This means that if the user requests more than the normal range, the IDS consider the user of the system is intended to carry out the attack. It should be considered that a violation of the threshold does not indicate the attack, alone. Because, when the network working under legal trafic, it is possible that the number of user packets be over the threshold and IDS blocked this user. We try to provide IDS based on the act of network users as well as the behavioral threshold to reveal the intrusion. When a user intend to send packets with a suspect total length, the IDS is activated and it can monitor the user.

Indian Journal of Science and Technology Vol. 5 No. 6 (June 2012) ISSN: 0974- 6846

At the moment, the behavior of the user stored in certain variables and if the user sends another request at next time range, the amount of time for the new packet is added to the total time variable. Then the system will compare this variable with the behavioral threshold. If it is higher, Users can be identified as the attacker and IDS blocked it.

Fig. 5. Network attack



Determining threshold

The easiest way for defining a threshold is to set the constant value for it. However, this is not an optimal slution, because the probability of false detection will be high. The important point is that this value should be chosen so that Possibility of false-negative detection (legitimate users rather than the attacker) is reduced. In our system, the threshold determined as a dynamic variable based on the network position and pressure traffic autmatically.

Challenge in implementation

In this paper, we implement an IDS and then applying DDoS attack on them, and evaluate the result of the atack. However, to achieve these goals, there are challenges that must be made appropriate decisions about them. These major challenges are how to generate traffic and the intelligence of the IDS under the attack.

In the manufacturing sector of attack traffic, it should be considered that the traffic is much closer to reality. In order to experiment with results could be cited. Another important point is that intelligence in the attack traffic. Attack should be implemented so that from the intelligence level is desirable. Any degree of intelligence and atacking from the more accurate the results will be higher. Because, the results would be more accurate if the degree of intelligence of the attack is higher.

Experimental result and solution

The cloud system which is implemented in this work has 10 MB band width, and each agent has 1MB band width. Fig. 5 shows a graph of network attacks in different situation. The graph is divided into several parts. In part A of this figure, the cloud system is act in normal mode. As this part show the cloud system reply to legal packet without any problem. In the beginning of part B, attack is started. As you could see in this part, the traffic rate in the cloud system is increased. In this time all agent start to send packet to the cloud. Thus the cloud sytem cannot be able to respond to the legal user. In the beginning of the part C, IDS become active, and start to count each user variable as described in section 4. In the next stage, with comparing this variable with the behavioral threshold, it detect agent as an attacker and it tries to block these agents. Finally, part D of Fig. 5, the cloud system is shown after detecting and blocking the attackers.

Detection of handler nodes in a DDoS attack is very difficult. Because, in this attack, many agents probably do not know that they used by the handler to attack. All these agents are control by different handlers, and the main attacker starts their attack even without a high band width. In these attacks, several important results should be noted. Finding of the main attacker node before the attack is nearly impossible. Therefore, the main attacker might start the new attack by different handlers and agents, again. Although, if an attacker can use many different networks to attack, even we could block them, that will be blocked the access of many legal users across the Iternet. Since the attacks take a long time. Consequently, the process of identifying and preventing would usually waste their own resource, which is associated with the system itself.

According the circumstances and results explained earlier, we propose few suggetions for the defense against DDoS attacks beside the IDS.

Load balancing

Distributing processing and communications activity evenly across a computer network so that no single dvice is overwhelmed (Anh Le *et al*., 2008). Load balancing is especially important for networks where it's difficult to predict the number of requests that will be issued to a server. Busy services typically employ two or more cloud servers in a load balancing scheme. If one server starts to get swamped, requests are forwarded to another serer with more capacities. Load balancing can also refer to the communications channels themselves.

Honey pot

A honeypot is as a closely monitored computing resource that we intend to be probed, attacked, or comprmised. The value of a honeypot is determined by the information that we can obtain from it (Anjali Sardana & Ramesh Joshi, 2009). Monitoring the data that enters and leaves a honeypot lets us gather information that is not available to IDS. To detect malicious behavior, IDS require signatures of known attacks and often fail to dtect compromises that were unknown at the time it was deployed. On the other hand, honeypots can detect vulnerbilities that are not yet understood. Because a honeypot has no production value, any attempt to contact it is suspicious. Consequently, forensic analysis of data collected from honeypots is less likely to lead to false postives than data collected by IDS.

Indian Journal of Science and Technology Vol. 5 No. 6 (June 2012) ISSN: 0974- 6846

Summary and conclusion

Our study is focused on investigating the effect of DDoS on the cloud system. After a short description of the cloud system and advantageous, Deployment Models of them, we pointed to the challenge of the cloud. We explain DDoS concept and design a model for an attack and IDS for defense for the cloud. Then, the model is simulated on a cloud with 10 MB band width with 12 agents and four handlers. The result of attack illustrated how the DDoS attack effect on the cloud. We prove that the attack could down the cloud system. For defense against DDoS attack in the real network (i.e the number of handler's and agents is more than my design model) several solutions are proposed. These are load balancing, honeypot and IDS.

Traffic of the cloud is distributed between network devices by Load balancing. Honeypots is proposed as another proposing solution to detect the signature of the attacker by analyzing of data collected. Therefore, the attacker is distinguished from legal customers. With utilizing of these proposed solutions with each other a cloud system might resist against DDoS attack.

References

1. Weiss A (2007) Computing in the Clouds. *Networker.* 11(4), 16-25.
2. Vidyanand Choudhary (2007) Software as a service: Implications for Investment in software development, hicss, pp.209a. 40th Annual Hawaii Int. Conf. Sys. Sci. (HICSS'07).
3. Bhaskar Prasad Rimal, Eunmi Choi, Ian Lumb (2009) A Taxonomy and survey of cloud computing sytems. Ncm. 5th Int. Joint Conf. INC, IMS & IDC. pp.44-51
4. Ian Foster, Yong Zhao, Ioan Raicu and Shiyong Lu (2008) Cloud computing and grid computing 360-Degree compared, *IEEE Grid Comput. Environ.* (GCE08) 2008, co-located with *IEEE/ACM Supercomputing*.
5. Luis M Vaquero, Luis Rodero-Merino and Daniel Morán (2011) Locking the sky: a survey on IaaS cloud security. *Comput.* 91(1), 93-118.
6. Amardeep Singh ER and Monika Verma ER (2011) Attacks and security in cloud computing. *Int. J. Adv. Eng. & Appl.* pp: 300-302.
7. Mihai Christodorescu, Reiner Sailer, Douglas Lee Schales, Daniele Sgandurra and Diego Zamboni (2009) Cloud security is not (just) virtualization security: a short paper. *Proc. 2009 ACM workshop on Cloud Computing Security (CCSW '09)*. ACM, NY, USA. pp: 97-102.
8. Jose Nazario (2008) DDoS attack evolution. *Network Security.* I7, 7-10.
9. Catteddu D and Hogben G (2009) Cloud Computing: benefits, risks and recommendations for information security. Technical Report. Europ. Network & Inforamtion Security Agency. pp: 9-30.
10. Victor Chang, David Bacigalupo, Gary Wills, and David De Roure (2010) A Categorisation of Cloud Computing Business Models. Proc. 10th IEEE/ACM Int. Conf. Cluster, Cloud & Grid Comput. (CCGRID '10). *IEEE Comput. Soc.,* Washington, DC, USA. pp: 509-512.
11. Basheer Al-Duwairi and Manimaran G (2009) JUST-google: a search engine-based defense against botnet-based DDoS attacks. Proce. *IEEE Int. Conf. Commun (ICC'09)*.
12. Christos Douligeris and Aikaterini Mitrokotsa (2003) DDoS attacks and defense mechanisms: classification and state-of-the-art, Elsevier B.V.
13. Asayuki Murakami and Nakaji Honda (2007) A study on the modeling ability of the IDS method: A soft coputing technique using pattern-based information processing. *Int. J. Approx. Reasoning.* 45(3), 470-487.
14. Anh Le, Raouf Boutaba and Ehab Al-Shaer (2008) Correlation-based load balancing for network intrusion detection and prevention systems. Proc. 4th Int. Conf. Security & Privacy in Commun. Networks (SecureComm '08).
15. Anjali Sardana and Ramesh Joshi (2009) An auto-responsive honeypot architecture for dynamic resource a location and QoS adaptation in DDoS attacked networks. *Comput. Commun.* 32, 121384-1399.