Analysis of Security Model for Cloud Computing against DDoS attack

Karnik Pooja Jagdish
Dept. of Computer Science and Engineering
Reva University
Bangalore, India
poojakarnik195@gmail.com

Jyoti Kiran Mirji
Dept. of Computer Science and Engineering
Reva University
Bangalore, India
jyotimirji@reva.edu.in

Shilpa Chaudhari
Dept. of Computer Science and Engineering
Reva University
Bangalore, India

Abstract

Cloud computing is a model for on demand network access to a shared pool of resources such as servers, storage, applications and related services. The six specific characteristics are common to the majority of cloud environments On-Demand Usage, Ubiquitous Access, Multi-tenancy (Resourcing Pooling), Elasticity (and Scalability), Measured Usage, Resiliency. Cloud computing is facing various attacks and danger from the hackers community and this has become the main hurdle in advancing of Cloud computing services. Today, distributed denial-of-service (DDoS) attack in Cloud computing is one of the major security concerns. This paper is an effort to put forth the types of DDoS attack and the prevention techniques. The paper also explains about the DDoS attack detection and mitigation techniques.

Introduction

Cloud computing is defined as the storage, management, processing, and accessing information and other data stored in a specific server. The “cloud” pertains to all these necessary information. Cloud Computing makes computer infrastructure and services available "on-need" basis.

Out of confidentiality, integrity and availability as three major issues in cloud security, availability is the area where cloud based infrastructure appears to have had its largest challenges to date; and it is Distributed Denial of Service (DDoS) attack, a major threat to availability. In cloud computing where infrastructure is shared by potentially millions of users, DDoS attacks have the potential to have much greater impact than against single tenanted architectures. Few popular attacks which gained lot of attention in the research community [Nelson 2015]. Cloud based gaming services of Microsoft and Sony were attacked by Lizard Squad which proved to be a fatal attack. Cloud service provider, Rackspace, was targeted by a massive DDoS attack on its services. In an another notable attack example, Amazon EC2 cloud servers were attacked by another massive DDoS attack.

Types of DDoS attacks :

1) *Volume Based Attack :*

Attackers keep sending requests to keep the server occupied to acquire bandwidth and break the link between the cloud resources & the consumers by creating a network traffic. The number of requests sent are more and may lead to overloading of the server.

2) *Protocol Attacks :*

The attackers try to distruct the load balancer & other firewalls which are meant for security check and lead to TCP state exhaustion. The security check is not possible and it becomes very easy for the attacker to apply a DDoS attack. The load balancer is unable to handle the huge number of requests and may lead to server breakdown.

3) *Application Layer Attacks :*

These are the most dangerous attacks as the attack rate is very slow & hard to detect. Flooding attacks like HTTP GET Flood is very common attack launched on the webserver in which the server must also serve the resource requests from the malicious attackers along with the legitimate users. As the resource requests from the malicious users is huge, the server is completely overloaded and it becomes nearly impossible to serve the legitimate user requests.

HTTP GET FLOOD uses tools like Slowloris & Rudy [1]. Slowloris is a kind of slow attack in which the attacker tries to bombard the victim server with as many connections as possible for a prolonged period of time by blocking the legitimate users from requesting for the resources. Another flooding attack is the DNS query flood, which is again a slow attack with the high intensions to damage the server by sending many resource requests. Even though the rate of these attacks exceed 200Gbps, the attack rate of 20 to 40 Gbps is enough to bring down the server completely.

DDOS flood in layer-3 attack include UDP flood and ICMP flood

1) *UDP Flood attack :*

The specific UDP ports of the server are purposely congested with UDP packets & when no application is waiting for that ports, it sends the message "destination unreachable" ICMP message to the source addresses.

2) *ICMP Flood attack :*

Many ICMP echo packets are sent to congest the server's bandwidth & the victim needs to reply all the echo requests. This generates a huge load on the server and leads to server shutdown.

It is possible to detect UDP and ICMP flood attacks [2] and can be easily prevented by setting the threshold limits to the routers sending UDP / ICMP packets.

Attack Prevention :

It is the need of the hour to understand and implement various strategies to prevent the above different types of attacks.

Following are the various DDoS attack prevention methods which can be used to control and prevent the DDoS attack to some extent.

Challenge Response Protocols :

It is mainly designed to check if the user is a bot / attacker machine.

The following are some important CRPs, which are used in traditional DDoS defense mechanism :

1) *Graphical Tests :*

Graphical Turing tests are done using graphical CAPTCHA which are moving images [4,5] in the form of .GIF or we need to choose a picture from multiple pictures provided. This image may be a picture or text with distortion or noise. This provides an effective method for identifying the bots and it is used in some of the areas where security is a concern. But the main problem is, it is difficult to generate graphics and requires more storage space for storing the images. Image segmentation and Optical Character Recognition (OCR) are the methods for CAPTCHA cracking [4,6]. They are prone to attacks by AI (Artificial Intelligence) bots.

2) *Text Puzzles :*

Text puzzles are purely textual questions with answers to be entered in the text box and may sometimes require answer to be chosen from question itself. Lexical Functional Grammars are used to construct natural language questions [7] which is difficult to answer by the machine using parsing and other techniques. Also there is a time duration to answer the questions which is approximately 3 seconds. But, this maybe cracked using dictionary attacks or parsing attacks. Accessibility is not considered during the question generation as it is easy to generate difficult questions for the bots but is equally important to realise that the questions should be answered by the normal users also with adequate comfort.

3) *Crypto Puzzles and Proof-of-Work :*

Crypto Puzzles are the questions with functions and input values, in which the user needs to answer by giving the proper output for that function within the stipulated time.

Proof-of-Work are crypto puzzles with advanced features to check the computational power of the client based on the correctness and time taken to solve the puzzle [9,13]. Based on that, the client is said to be authentic and access is granted. This makes it easy to assess the computational capability of the client and depending on the time taken to solve the puzzle it is easy to determine if the incoming request traffic is legitimate traffic or not. There are many levels of difficulty available for the puzzles to identify the legitimate customers [9,10,11]. Attaker may request for getting large number of puzzles but does not solve them which leads to an overload for generating these puzzles at the server side [12]. It is difficult to prepare puzzles with unique solutions with the server being capable enough to compute the answers [3].

Other Prevention Methods :

1) *Hidden Servers / Ports :*

It is a preventive mechanism to save the real server to face a DDoS attack. The resource requests go to the hidden proxy servers [13] which are then redirected to the authentication servers [9] for providing extra security to the real servers from DDoS attacks. The extra security layer supports in redirection and load balancing among the servers. Many hidden proxy servers are dynamically assigned and changed in order to save the legitimate clients. Attackers are distinguished from the normal traffic via client puzzles using Proof-of-Work. It is possible to shuffle the target servers by creating the server replicas to confuse the attackers [14]. Request rate based detection method can be used in which the request rate must never exceed the threshold rate which will help in serving the legitimate clients. There is an overhead of an extra security layer. There is a problem of scalability, including large number of proxy servers and their shuffling. There is an overhead for the web services with changing server addresses in between the connection establishment.

2) *Delayed Access :*

Delaying the access to the suspected attacker is another effective method to prevent the DDoS attacks which helps in prioritizing the legitimate clients. Delayed access prevents attack and even auto scaling [15]. Human behavior based identification [16] to prevent the attacker requests to block the attacker for some period of time and then again unblock is possible. There are many user accessibility issues which requires timely responses. The home page of the website is free from puzzle or authentication and are targeted for a DDoS attack.

3) *Selective Access :*

This is a preventive method which allows only specific clients to access the resources based on actual capacity. Admission control algorithm [17] is used to allow only those legitimate users who have cleared the turing test within the stipulated time. This method helps to filter out the excess requests and benign requests but is not useful for user driven business web sites as it has an adverse effect on the conversion rates.

4) *Reputation based Access :*

It is similar to selective access in which the users with high reputation are serviced [9]. This reputation is obtained by solving the crypto puzzles correctly in a definite time and also based on the past web access behavior. In this case, new requests are not handled properly and spoofing can crack the defense mechanism used.

5) *Resource Limits :*

Providing resource limits in the form of "Caps" on maximum resources a VM can sustain and beyond this limit, the resource request is not accepted by the server [18]. This method helps in billing limits and there is lesser burden of downtime. But, this does not prevent DDoS attacks and only prevents the economic losses.

Attack Detection :

Attack detection method is the presence of attack signs on the server based on change in the services and performance. Performance metrics monitor the response time and time outs and even memory and CPU usage.

Following are the different attack detection methods which can be used :

Pattern Detection :

To identify a certain pattern in client's web access behavior by the access logs or request headers.

Various types of pattern detection methods include:

1) *Anomaly Detection :*

Legitimate web access pattern follow "Zipf" distribution [19,22] but the attacker can be easily identified as he fails to follow this distribution pattern.

The Zipf's law states that :

Frequency of the web page request is inversely proportional to the rank of the particular page.

Statistical filtering [20] based attack detection helps to calculate the divergence between the normal and attacker traffic using the Jensen-Shannon Divergence [21]. After the IP spoofing, the anomalies in the traffic is identified using the divergence method which provided nearly an attack detection accuracy of 97%. It is easy to detect the normal or the attacker traffic using Jensen-Shannon divergence but there is an overhead of statistical anaysis of traffic.

2) *Session Duration :*

Indicates the amount of time spent on web sessions [22,23]. The attackers Time Spent on a Page (TSP) [23] is mostly near to zero as they would use the page only for flooding and even if it is not zero then, it is constant or periodic. TSP helps to filter out the legitimate users from attackers. IP Spoofing and scalability issues are the major drawbacks of this method.

3) *Web Behaviour :*

Detecting the HTML DoS and XML DoS is possible by training the system for typical SOAP requests which helps in identifying the attackers [8]. Through the websites of an e-commerce site, it is possible to detect the attackers based on the priority. A high priority is given to the customer who frequently makes a purchase and low priority to the one who merely visits the site and even if visited does not make any purchase but in turn applies higher load queries [17]. This method helps statistical pattern to detect the web sessions. There is an overload to keep a track on the traffic metrics.

4) *Source / Spoof Trace :*

Trace back algorithm is used to stop spoofing by finding its source and back propagation neural networks to tackle the DDoS attacks. Egress filtering [24] is used to drop all the spoofed packets at edge routers. Real web server is placed after the additional server which is known as Service-Oriented-Architecture - Based Trace back Approach. It marks each packet with trace back tag and even traces the path to find the source. These trace back tags are placed in database and fetched as and when required for tracing its source. Spoofing can be identified by matching the OS versions of the attacker and the real IP owners and OS fingerprint [25] of the spoofed attacker can be obtained. This helps in source authentication by verifying the cryptographic tokens [26]. Support from various network devices and services is very difficult.

4) *BotCloud Detection :*

Cloud infrastructure is used for installing botnets. Network level checks are done to identify the attacker bots running inside VMs [27]. Virtual Machine Introspection (VMI) [28] and data mining techniques are involved in separating the infected VMs from the other VMs in multi-tenant architecture. Based on the level of training provided to the clustering algorithms, they are used to identify the malware bots infected VMs.

Threshold Filtering :

Threshold filtering is done to identify the initialization of the attack and later to identify the presence of attack on suspicious VMs.

1) *Hop Count Based :*

Attacker packets are identified if they have the same hop count [8]. TTL values depending on IP addresses are classified as black or white list. In case of any new incoming request or presence of different TTL value [11] for the one present in any of the lists, is made to pass through the Turing test and only after the verification, they are included in the list and the TTL value is updated. Hop count based filtering method is successful only if dissimilar TTL values from the same IP source is obtained.

2) *Request Count Based :*

Request count of the user must be always less than the threshold value. It is easy to identify DDoS attacks by multiple level filtering [8] based on client puzzles, hop count and packet frequency.

Overhead of maintaining various filters at the server side and the latency period for the legitimate users. IP Spoofing can defeat this mechanism.

Attack Mitigation :

1) *Migration :*

Running server is shifted to another physical server which is isolated from any kind of attack without noticeable downtime [29]. After the recovery from the DDoS attack, the server can be again restored at its original location [27]. This creates minimum economic loss but generates downtime to legitimate customers and may lead to heavy migration costs.

2) *Shutdown :*

We can shutdown the attacked proxy servers and redirect the traffic to the new proxy servers [13]. This is a quick defense mechanism but there is no solution to the downtime of the service and business reputation is degraded.

3) *Backup Resources :*

Dynamic resource allocation is made to provide the victim server with additional resources for DDoS mitigation. The Virtual Machine Monitor [29] detects the possibility of DDoS attacks by continuously monitoring the resource utilization levels. The major drawback is that, additional resources as backup must be available all the time. There is redundancy of the resources which cannot surpass heavy traffic congestions and leads to heavy backup cost [30].

Table1: Types of DDoS Attack and the prevention methods.

Types of DDoS attack	Volume Based Attack	Protocol Attacks	Application Layer Attacks	Layer-3 attack	
Attack Prevention				UDP Flood attack	ICMP Flood attack
Graphical Tests	√		√		
Text Puzzles			√		
Crypto Puzzles and Proof-of-Work		√		√	√
Hidden Servers / Ports		√	√		
Delayed Access	√	√	√	√	√
Selective Access			√		
Reputation based Access			√		
Resource Limits	√	√		√	√

In the above Table1 we have listed some of the DDoS attacks and the preventive methods. The Graphical test can be used to prevent the Volume based attack and application layer attacks. Text Puzzles can prevent the protocol attack and UDP, ICMP flood attacks. Crypto Puzzles and Proof-of-work can avoid protocol and layer 3 attacks. Hidden Server/Ports prevent protocol attack and layer-3 attack. Delayed Access to the server can prevent most of the DDoS attacks. Selective and Reputation based access can prevent the application layer attack. By having the limitation on the resources we can prevent volume based, protocol, application, layer3 attacks.

Conclusion

In this paper we have discussed some of the attacks on cloud. More stress is given on the DDoS attacks. The different types of DDoS attacks have been discussed. Some of the preventive techniques for DDoS attacks have been briefed.

Full proof prevention of attack is not possible, hence if there is an attack in cloud, it has to be detected. Some of the DDoS attack detection techniques have been discussed. And also some of the mitigation methods have been briefed.

Further work can be done by analyzing some more mitigation methods and can be implemented.

References :

[1] Junath Naseer Ahamed and N.Ch.S.N.Iyengar, "A Review on Distributed Denial of Service (DDoS) Mitigation Techniques in Cloud Computing Environment", vol. 10, No.8 (2016), pp.277-294.

[2] A. M. Sharifi, S. K. Amirgholipour, M. Alirezanejad, B. S. Aski and M. Ghiami, "Availability challenge of cloud system under DDoS attack", vol. 5, no. 6, (2012), pp2933-2937.

[3] David Leggett. 2009. CAPTCHAs tough on sales common way to test user tolerance. http://www.uxbooth.com/articles/captchas-tough-on-sales-common-way-to-test-user-tolerance/. (2009).

[4] William G. Morein, Angelos Stavrou, Debra L. Cook, Angelos D. Keromytis, Vishal Mishra, and Dan Rubenstein. 2003. Using Graphical Turing Tests to Counter Automated DDoS Attacks Against Web Servers. In Proceedings of the 10th ACM Conference on Computer and Communications Security (CCS'03). ACM, New York, NY, USA, 8-19. DOI : http://dx.doi.org/10.1145/948109.948114

[5] Jeff Yan and Ahmad Salah El Ahmad.2009. Captcha

security : A case study. IEEE Security and Privacy 7, 4 (2009), 22-28.

[6] Abliz and T. Znati. 2009. A Guided Tour Puzzle for Denial of Service Prevention. In Computer Security Applications Conference, 2009. ACSAC'09 Annual. 279-288. DOI : http://dx.doi.org/10.1109/ACSAC.2009.33

[7] VS Huang, Robert Huang, and Ming Chiang. 2013. A DDoS Mitigation System with Multi-Stage Detection and Text-Based Turing Testing in Cloud Computing. In Advanced Information Networking and Applications Workshops (WAINA), 2013 27th International Conference on. IEEE, 655-662.

[8] Tarun Karnwal, T Sivakumar, and G Aghila.2012. A comber approach to protect cloud computing against XML DDoS and HTTP DDoS attack. In Electrical, Electronics and Computer Science (SCEECS), 2012 IEEE Students' Conference on. IEEE, 1-5.

[9] Soon Hin Khor and Akihiro Nakao. 2009. spow: On-demand cloud-based EDDoS mitigation mechanism. In HotDep (Fifth Workshop on Hot Topics in System Dependability).

[10] Madarapu Naresh Kumar, P. Sujatha, Vamshi Kalva, Rohit Nagori, Anil Kumar Katukojwala, and Mukesh Kumar. 2012. Mitigating Economic Denial of Sustainability (EDoS) in Cloud Computing Using In-cloud Scrubber Service. In Proceedings of the 2012 Fourth International Conference on Computational Intelligence and Communication Networks (CICN'12). IEEE Computer Society, Washington, DC, USA, 535-539. DOI : http://dx.doi.org/10.1109/CICN.2012.149

[11] Fahd Al-Haidari, Mohammed H. Squalli, and Khaled Salah. 2012. Enhanced EDoS-Shield for Mitigating EDoS Attacks Originating from Spoofed IP Addresses. In the 11th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom 2012, Liverpool, United Kingdom, June 25-27, 2012, Geyong Min, Yulei Wu, Lei (Chris) Liu, Xiaolong Jin, Stephen A. Jarvis, and Ahmed Yassin Al-Dubai (Eds.). IEEE Computer Society, 1167-1174.

[12] Mohammed H. Squalli, Fahd Al-Haidari, and Khaled Salah. 2011. EDoS-Shield - A Two-Steps Mitigation Technique against EDoS attacks in Cloud Computing. In UCC. IEEE Computer Society, 49-56.

[13] Huagxin Wang, Quan Jia, Dan Fleck, Walter Powell, Fei Li, and Angelos Stavrou. 2014. A moving target DDoS mechanism. Computer Communications 46 (2014), 10-21.

[14] Quan Jia, Huangxin Wang, Dan Fleck, Walter Powell. 2014. Catch Me If You Can : A Cloud-Enabled DDoS Defense. In Dependable Systems and Networks (DSN), 2014 44th Annual IEEE/IFIP International Conference on. IEEE, 264-275.

[15] Zubair A. Baig and Farid Binsher. 2013. Controlled Virtual Resource Access to Mitigate Economic Denial of Sustainability (EDoS) Attacks Against Cloud Infrastructures. In Proceedings of the 2013 International Conference on Cloud Computing and Big Data (CLOUDCOM-ASIA'13). IEEE Computer Society, Washington, DC, USA, 346-353. DOI : http://dx.doi.org/10.1109/CLOUDCOM-ASIA.2013.51

[16] Bhavna Saini and Gaurav Somani. 2014. Index Page Based EDoS Attacks in Infrastructure Cloud. In Recent Trends in Computer Networks and Distributed Systems Security. Springer, 382-395.

[17] Masood, Z. Anwar, S.A. Raza, and M.A. Hur. 2013. EDoS Armor : A cost effective economic denial of sustainability attack mitigation framework for e-commerce applications in cloud environments. In Multi Topic Conference (INMIC), 2013 16th International. 37-42. DOI: http://dx.doi.org/10.1109/INMIC.2013.6731321

[18] AWS Discussion Forum. 2006. https://forums.aws.amazon.com
https://forums.aws.amazon.com (2006).

[19] Joseph Idziorek, Mark Tannian, and Doug Jacobson. 2011. Detecting fraudulent use of cloud resources. In Proceedings of the 3rd ACM workshop on Cloud computing security. ACM, 61-72.

[20] Shamsolmoali et al. 2014. Statistical-based filtering system against DDoS attacks in cloud computing. In Advances in Computing, Communications and Informatics (ICACCI), 2014. International Conference on. IEEE, 1234-1239.

[21] Juan Francisco Gomez-Lopera, Jose Martinez-Aroza, Aureliano M Robles-Perez, and Ramon Roman-Roldan. 2000. An analysis of edge detection by using the Jensen-Shannon divergence. Journal of Mathematical Imaging and Vision 13,1 (2000), 35-56.

[22] Joseph Idziorek and Mark Tannian. 2011. Exploiting Cloud Utility Models for Profit and Ruin. In Proc. IEEE International Conference on Cloud Computing (4th IEEE CLOUD'11). IEEE Computer Society, Washington, DC, USA, 33-40.

[23] Koduru, T. Neelakantam, and S.M. Saira Bhanu. 2013. Detection of Economic Denial of Sustainability Using Time Spent on a Web Page in Cloud. In Cloud Computing in Emerging Markets (CCEM), 2013 IEEE International Conference on. 1-4. DOI : http://dx.doi.org/10.1109/CCEM.2013.6684433

[24] Lanjuan Yang, Tao Zhang, Jinyu Song, JinShuang Wang, and Ping Chen. 2012. Defense of DDoS attack for cloud computing. In Computer Science and Automation Engineering (CSAE), 2012 IEEE International Conference on. Vol. 2. IEEE, 626-629.

[25] Opeyemi Osanaiye and others. 2015. IP spoofing detection for preventing DDoS attack in Cloud Computing. In Intelligence in Next Generation Networks (ICIN), 2015 18th International Conference on. IEEE, 139-141.

[26] Mirkovic, G. Prier, and P. Reiher. 2002b. Attacking DDoS at the source. In Network Protocols, 2002. Proceedings. 10th IEEE International Conference on. 312-321. DOI : http://dx.doi.org/10.1109/ICNP.2002.1181418

[27] Joseph Latanicki, Philippe Massonet, Syed Naqvi, Benny Rochwerger, and Massimo Villari. 2010. Scalable Cloud Defences for Detection, Analysis and Mitigation of DDoS Attacks. In Future Internet Assembly. 127-137.

[28] Reza Memarian Mohmmad, Conti Mauro, and Leppanen Ville. 2015, EyeCloud : A BotCloud Detection System. In Proceedings of the 5th IEEE International Symposium on Trust and Security in Cloud Computing (IEEE TSCloud 2015), Helsinki, Finland. IEEE.

[29] Siqin Zhao, Kang Chen, and Weimin Zheng. 2009. Defend against denial of service attack with VMM. In Grid and Cooperative Computing, 2009. GCC'09. Eighth International Conference on. IEEE, 91-96.

[30] Gaurav Somani, Manoj Singh Gaur, Dheeraj Sanghi, Mauro Conti, Rajkumar Buyya, "DDoS Attacks in Cloud Computing : Issues, Taxonomy, and Future Directions", vol.1, No. 1, Article 1, Publication date : December 2015.