ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645
Indian Journal of Science and Technology, *Vol 9(47), DOI: 10.17485/ijst/2016/v9i47/106903, December 2016*

Reducing DDoS Attack in Cloud using Layered Model

N. Sharma and P. K. Pateriya

School of Computer Science and Engineering, Lovely Professional University, Phagwara – 144411, Punjab, India; nehasharma.ns12@gmail.com, pushpendra.14623@lpu.co.in

Abstract

Background: Cloud Computing is the field of concern these days. Organizations are more worried for the security of cloud as it provides resources on "pay-as-you-need" basis. **Methods**: Security and safety are the two most important things in cloud. An enhanced model is proposed to detect the DDoS attack. The model consists of many phases which will filter out the attack at each layer. **Findings**: The system is proposed with different layers namely IP address filtering which will filter the illegitimate ip addresses followed by hop count check. Cloud Traceback Model is used as one layer which uses the technique of marking the packets and is capable of filtering the packets. **Applications/ Improvements:** The model proposed is applicable in cloud infrastructure as it embeds different techniques to reduce the chances of DDoS attack. The model is easy to deploy and all the modules can be easily integrated into one model.

Keywords: Cloud Computing, DDoS, Encryption, Hop count , Legitimate IP, Trace Back Model

1. Introduction

Cloud computing can be defined as the online services provided to users on 'as-need' basis. It provides infrastructure which is inexpensive and is easily accessible from anywhere in this world. It is becoming a heart of resource sharing and moving gigantic data, applications onto a third party service i.e cloud and then using it in simple and flexible manner[1]. The basic structure of cloud[2] is shown in Figure 1.

The different layers or hierarchical arrangement[2] is seen as IaaS, PaaS and SaaS as shown in Figure 2. According to the cloud users, the services are classified as SaaS, PaaS or IaaS. The users need not to worry about the internal arrangement of the cloud. Any kind of disruption seems to the cloud users either as service unavailability or quality deterioration. It's a challenge to overcome this deterioration. Security issues exist and play a very crucial part for any cloud user. Security is the major aspect of cloud computing as cloud computing encounters many users and their sensitive information. Hence authentication and integrity plays an important role along with securing such credentials in cloud environment.

But today most of the companies and organizations are reluctant to store their data on cloud as it is open and is thus vulnerable to attack[3]. User doesn't know where the data is stored. Data is stored on a third party virtual cloud so it is not always guaranteed that your data is secured. That is why organizations generally refuse to store data on cloud. Thus cloud computing suffers from various challenges in the field of availability, security, performance, integrity and cost factors. Availability is the area with greatest threats and it is Distributed Denial of Service[4].

This paper presents a layered model for detection and filtering of DDoS attack at different layers with different techniques. Section 2 gives the characteristics of cloud which are posing a threat to security. Section 3 presents the security of cloud. Section 4 presents the overview

*Author for correspondence

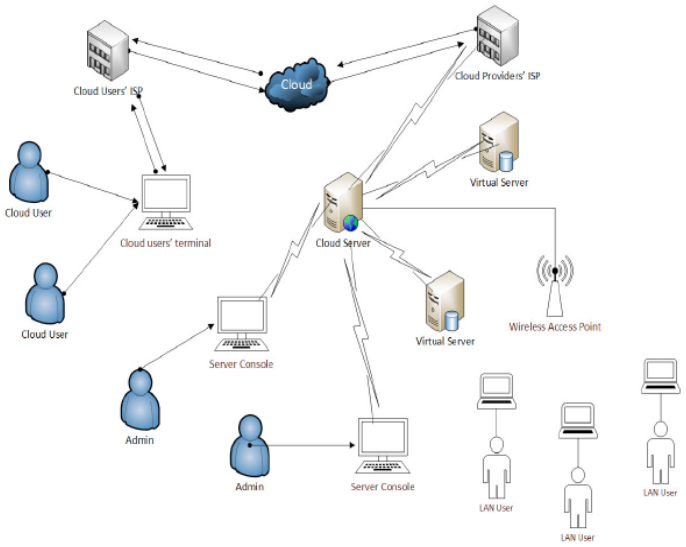

Figure 1. Basic cloud structure[2].

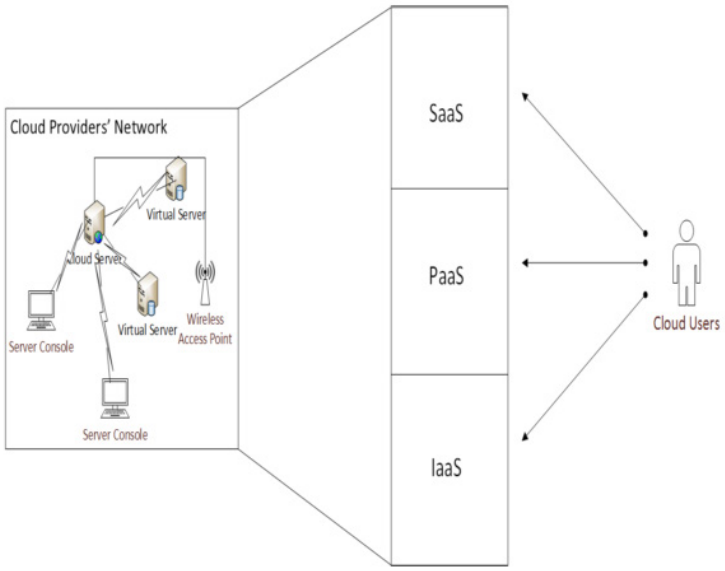

Figure 2. Cloud service[2].

of the famous techniques used, section 5 provides the overview of proposed model and section 6 provides the working of the layered model. Ultimately, section 7 gives the conclusion of this paper.

2. Cloud Characteristics for Security

Different characteristics of cloud include multi-tenancy, elasticity, multiple stakeholders and third party control.

Multi-tenancy promotes many kinds of threats related to confidentiality and privacy[5]. Multi-tenancy in cloud means giving resources and services simultaneously to much number of users securely. And for this there is a risk that multiple users share same resources which can be a potential threat.

Security is one of the major concerns for using cloud today. Availability in cloud is the most challenging area right now as it is vulnerable to Distributed Denial of Service attack[6]. DDoS attack makes the resources in cloud unavailable to the legitimate users for the specified period of time[7]. At that very moment, the attacker retrieves the sensitive information and can perform some malicious attack. As the attacker spoofs the IP so it is difficult to recognize the legitimate IP from which the request comes.

One solution was introduction of the trusted third party[3]. The security parameter for cloud also includes cryptography mainly public key cryptography along with Lightweighted Directory Access Protocol (LDAP) which provides authentication and security and integrity over communication.

3. Security of Cloud

Cloud environment is having three types of cloud namely private cloud, public cloud and hybrid cloud[8] as shown in Figure 3 . Each is having different kinds of threats based on the services they offer. Private cloud is quite secure as it is used by the private organization whereas public cloud is more vulnerable to attacks.

Service based intrusion prevention system[9] is used to reduce the number of intrusions in a system. This technique works on three different modules namely client, server and open source host based intrusion detection system. Many different techniques are used to secure cloud environment which are discussed in the next section. Another mitigation technique is using SDN advantages (Software-Defined Networking)[10,11] DDoS attack can be handled somehow. Another method is Minutiae Map (MM) algorithm [12] which was implemented for processing fingerprint based authentication. The user personal files are stored in free public multiple cloud storages namely Dropbox and CloudMe using splitting and merg-

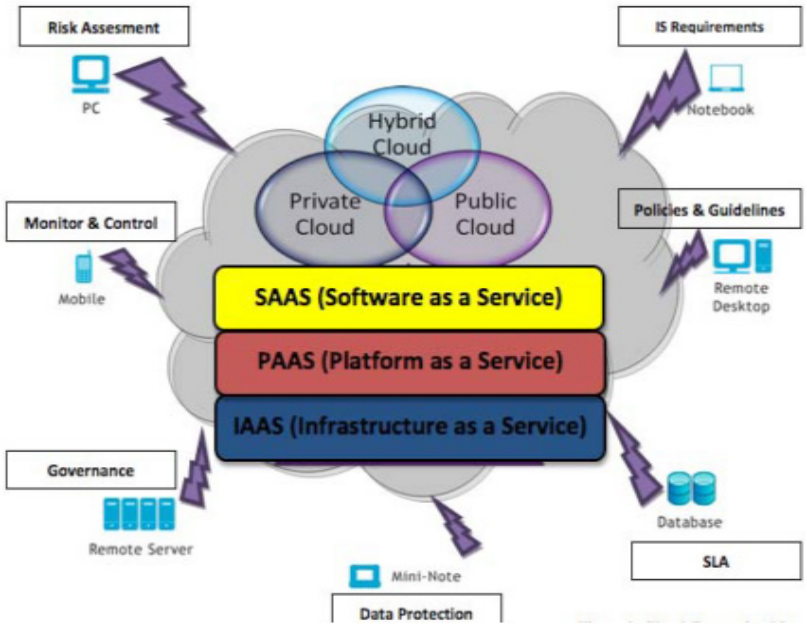

Figure 3. Types of cloud[8].

ing techniques. Even in biometric research group is very much concentrating on security of biometric templates. For the security of biometric template, the two encryption algorithms such as Advanced Encryption Standard (AES), Rivest-Shamir-Adleman (RSA) have been imposed on templates[13].

4. Overview of Techniques used in the Proposed Model

This section includes the overview of techniques at each layer and the working of the layered model.

4.1 Cloud Trace Back Mark

CTB mark is used to trace back the source of DDoS attack. Cloud trace back model is based upon flexible deterministic packet marking algorithm[14]. FDPM marks the packet and the marked packet does not undergo changes when it traverses in the network. FDPM mark length is dependent on the type of network that needs to be protected and its protocols on which it is working. The length my vary from 16-24 bits[15,16]. CTB is placed behind the servers so as to prevent the direct attack and to recognize the source of attack. When the request for any service is made, it first goes to the CTB placed before the server as shown in Figure 4, is marked and further if it were to cause any attack or has already made server down, then the victim will request to extract the mark and to find the source of attack.

4.2 Hop Counting

Hop count refers to the number of routers or network devices in between the path through which packet

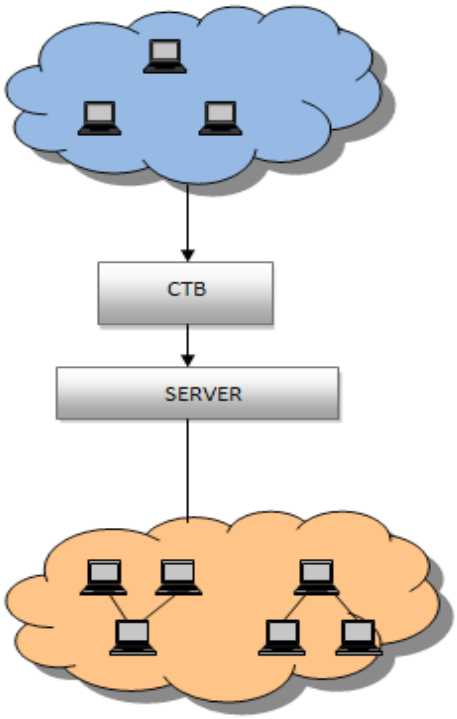

Figure 4. The cloud trace back model.

traverses before reaching the destination. Hop count generally determines the distance which packet moved.

Each packet is defined with a hop limit which represents time to live (ttl). If an attacker needs to modify packet, he cannot change the hop count value of the packet in the IPV6 header. Generally the maximum hop count of the system cannot exceed 255. The packet having same hop count and having same destination router are marked with some ID[17] which is the combination of 32bits IP address and the encrypted value of hop count. This ID is checked with the already stored values- if they matched then no attack, but if they don't then the chances of DDoS attack are more prominent.

4.3 Packet Encryption

Encryption means hiding data from the illegitimate users. Various Encryption techniques are used these days- feistel cipher, AES, Data Encryption Standard (DES) and many more. At the destination or the routers packets which are delivered are in encrypted form. When an attacker spoofs the IP address and sends a malicious packet, he is unaware of the encrypted technique used. Thus when the malicious packet is sent it is checked at server and is discarded if the encrypted format is not correct. Moreover the result will not be in an encrypted manner that simply indicates the presence of DDoS attack.

5. Proposed Model

The model consists of four layers namely- legitimate IP, Hop count, CTB and encryption. These layers filter the packets and determine whether it has been compromised or has undergone DDoS attack. When a packet arrives at first layer IP of the host is verified through which the packet comes and checks if it is legitimate or not. Packets cross the next layer which counts number of hops through which packet routes. After filtering at this layer, next layer filters packet based on the mark generated by FDPM and after that packets are verified by checking for proper encryption.

6. Working of Proposed Layered Model

First layer filters out the illegal IPs through which packet comes. This layer will check the already stored IPs with the one through which packet comes. If the packet is having the authorized IP then only it will allow the packet to pass otherwise will filter out the attack traffic. Thus it reduces chances of attack by just filtering out the illegitimate addresses.

At Second layer, some of the packets are already discarded and if anyhow the attacker passes the first filter then another check is applied on it i.e. Hop Count as shown in Figure 5. Hop count of the packet arriving is checked. If the hop count is legitimate then only the packet is allowed to pass through the network confirming that there is no kind of attack and the packet has come in an authorized manner.

If the packet hop count doesn't matches with the fixed hop count then the problem occurs and the packet is discarded. Packets are discarded intimating that it could cause DDoS attack in future.

If somehow attacker manages to penetrate malicious packet or try to bot other nodes then third layer comes in i.e. Cloud Trace Back Model. CTB marks the packet which is called Cloud Trace Back Mark (CTM). In CTB framework, this mark is kept in a web service message[18]. This mark will check each incoming packet to the ingress router. If any malicious behavior is encountered, the victim requests to reconstruct the mark. FDPM marking scheme encodes the mark and contains a recognition procedure to analyze the mark and trace back to the source of DDoS attack.

Trace back models can be implemented in intrusion detection systems, forensic systems and many more. Hence this layer will allow to check for DDoS attack and also to identify the origin of the message. Malicious or illegitimate IPs are filtered out and the rest goes to the next and the last layer of the model i.e. packet Encryption.

This layer would prevent attacks inside a network when the malicious message has entered the network.

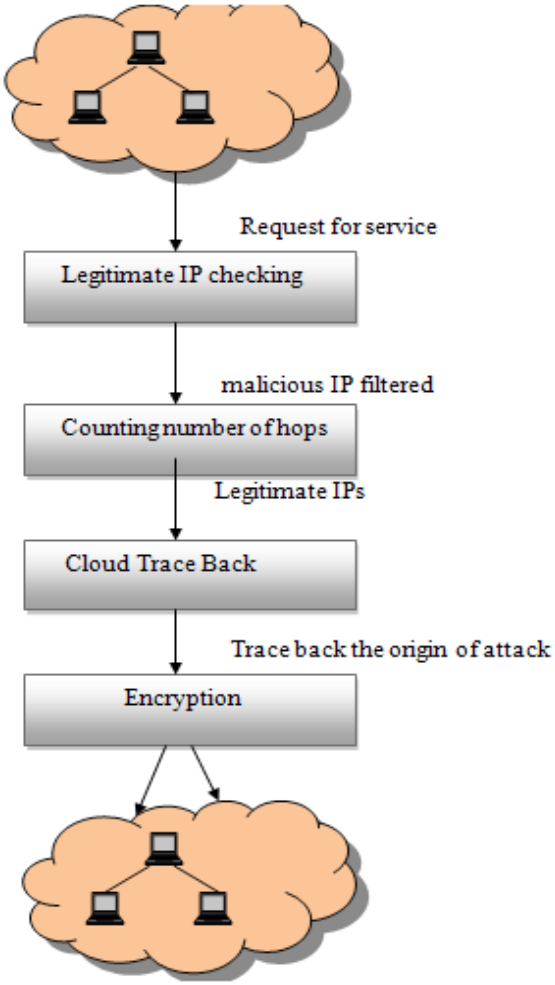

Figure 5. Proposed layered model for DDoS mitigation.

The router will check for the message if the message is correctly encrypted or not. If the message received is not encrypted that means something wrong occurred and it may cause DDoS attack i.e. slow down the server for the entire network.

7. Conclusion

Cloud is really a big term to use now-a-days. It's easy to do DDoS attack on cloud[19] but it's not easy for the security analysts and experts to mitigate these attacks as there is no way to know where data is stored. Thus this proposed model describes a simple way how to detect for any malicious behavior like DDoS attack in cloud infrastructure. It is observed that request coming from the users first is checked for the legal IP address and filters out the illegitimate IPs. Further security is provided by counting number of hops required for the transmission of the packet. It removes the packets whose count values are not as expected and thus reduce the vulnerabilities of attack to major extent. Further the paper deals with the cloud trace back model which uses FDPM to trace back the source in case of attack[14]. Last and most important is the Encryption of the message which checks that if the requested service is sent in encrypted form or someone has intruded in between and has changed the configuration.

This model will help to detect DDoS attack at different levels and filter out the vulnerabilities.

8. References

1. Wang L, Laszewski G Von, Younge A, He X. Cloud computing: A perspective study. New Gener Comput. 2010; 28(2):137–46.
2. Ahmed M, Hossain MA. Cloud Computing and Security Issues in the Cloud. International Journal of Network Security and Its Applications. 2014; 6(1):25–36. DOI:10.5121/ijnsa.2014.6103.
3. Zissis D, Lekkas D. Addressing cloud computing security issues. Future Generation Computer Systems. 2012; 28(3):583–92. DOI:10.1016/j.future.2010.12.006.
4. Bouzida Y, Cuppens F, Gombault S. Detecting and reacting against distributed denial of service attacks. 2006 IEEE International Conference of Communication ICC 2006. 2006; 5(August 2016):2394–9. DOI:10.1109/ICC.2006.255128.
5. Tianfield H. Security issues in cloud computing. IEEE International Conference on Systems, Man and Cybernetics. 2012:1082–9. DOI:10.1109/ICSMC.2012.6377874.
6. Popovic K, Hocenski Z. Cloud computing security issues and challenges. Proceedings of 33rd Interational Convention. 2010.p. 344–9.
7. Deshmukh RV, Devadkar KK. Understanding DDoS attack and its effect in cloud environment. Procedia Computer Science. 2015; 49(1):202–10. DOI:10.1016/j.procs.2015.04.245.
8. Ramgovind S, Eloff MM, Smith E. The management of security in Cloud computing. Information Security for South Africa. 2010:1–7.
9. Thesis M. Security solutions for cloud technologies. 2013;128(16):8887.
10. Yan Q, Yu FR, Member S, Gong Q, Li J. Software-Defined Networking (SDN) and Distributed Denial of Service (DDoS) Attacks in Cloud Computing Environments : A Survey , Some Research Issues , and Challenges. IEEE Commun Survey and Tutorials. 2015; 18(c):2–23. DOI:10.1109/COMST.2015.2487361.
11. Yan Q, Yu FR. Distributed denial of service attacks in software-defined networking with cloud computing. IEEE Communication Magazine. 2015; 53(4):52–9. DOI:10.1109/MCOM.2015.7081075.
12. Srinivasan S, Raja K. Preventing Cloud Attacks using Bio-Metric Authentication in Cloud Computing. 2016; 9(June). DOI:10.17485/ijst/2016/v9i23/88322.
13. Hari SK, Sudhan H, Kumar SS. An Innovative Proposal for Secure Cloud Authentication using Encrypted Biometric Authentication Scheme. 2015; 8(December). DOI:10.17485/ijst/2015/v8i35/82743.
14. Chonka A, Zhou W, Xiang Y. Protecting web services with service oriented traceback architecture. Proceedingsof IEEE 8th International Conference on Computer and Information Technology CIT 2008. 2008:706–11. DOI:10.1109/CIT.2008.4594761.
15. Belenky A, Ansari N. Tracing multiple attackers with deterministic packet marking (DPM). 2003 IEEE Pacific Rim Conference Communications, Computers and Signal Process (PACRIM 2003). 2003;1:49–52. DOI:10.1109/PACRIM.2003.1235716.
16. Degree B, Information IN. Flexible Determinisic Packet Marking : An IP Traceback System To Find Real Source Of Attack. 2009; 20(5):1–14.
17. Joshi B, Vijayan a. S, Joshi BK. Securing cloud computing environment against DDoS attacks. 2012 International Conference on Computer Communication and Informatics. 2012:1–5. DOI:10.1109/ICCCI.2012.6158817.
18. Chonka A, Xiang Y, Zhou W, Bonti A. Cloud security defence to protect cloud computing against HTTP-DoS and XML-DoS attacks. Journal of Network and Computer Applications. 2011; 34(4):1097–107. DOI:10.1016/j.jnca.2010.06.004.
19. Yu S, Tian Y, Guo S, Wu D. Can We Beat DDoS Attacks in Clouds?(Supplementary Material). IEEE Transactions on Parallel and Distributed Systems. 2000; 25(9):1–4. DOI:10.1109/TPDS.2013.181.