International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2020): 7.803

Protection of Cloud Servers from DDOS Attacks using DAM Servers

Nadesh S[1], Suriya K[2], Ashwin A[3]

[1, 2]SRM Valliammai Engineering College - Kattankulathur, Kanchipuram, Tamil Nadu, India
[3]Rajalakshmi Institute of Technology - Kuthambakkam, Chennai, Tamil Nadu, India

Abstract: ***Cloud computing is a booming service that is offered to customers and it is made available in many forms for the users. Some examples of these include cloud storage services and virtual computing. A denial - of - service attack (DoS attack) or distributed denial - of - service attack (DDoS attack) is an attempt to make a computer resource unavailable to its intended users. Cloud services are vulnerable to such serious attacks because of the nature of the service they provide. In this paper, various existing methodologies to prevent the denial - of - service attack (DoS attack) or distributed denial - of - service attack (DDoS attack) are analysed with respect to the performance and the quality of service they intend to provide to the customers. This paper will include the disadvantages of using the already existing techniques to prevent DDOS with respect to the cloud environment and proposing a technique of "DAM servers" which effectively reduces the DDoS attacks rather than presently available filtering approaches***.

Keywords: Cloud computing, Virtualization, Denial of service (DOS), Distributed Denial of service (DDOS), Filtering, Mitigation

1. Introduction

Cloud computing is an evolving and on - demand field in technology. It includes both what is delivered as a service over the internet and the hardware behind those services. Cloud computing has become a highly demanded service due to the advantages like Availability, Scalability, Agility and high computing power which are respectively cheap. In a Cloud network, users do not own the computing servers. They can access numerous services without the burden of Cloud management and their data can be accessed by way of many devices. On the other hand, security in cloud computing needs to be taken more seriously because these services handle the data of customers directly. Data leaks and irregular services are not acceptable as these will directly affect the customer and the reputation of the service which is intended to be secure and scalable.

DOS and DDOS will be a direct threat to these kinds of services because they will affect the stability of the service along with a direct threat to the reputation of the service. There are two ways in which a DOS/DDOS attack can happen in a cloud network. The ones that crash various resources and those that flood different services in the environment. The intention of these attacks are usually to damage the reputation of the service provider, however, the main aim of the attacker is unknown in most cases.

There exist many ways to prevent these attacks which are effective in some cases while it stays ineffective in most cases related to the cloud environment because service providers in cloud environments have to consider many things before deploying a solution to counter these attacks. Since cloud storage handles large data requests, the previously existing filtering techniques tend to be useless in this environment. A new methodology is proposed in this following paper to prevent these Attacks.

2. Problem Statement

Cloud services usually receive and compute a lot of requests in the form of data or instructions from the customer; these connections with cloud resources are vulnerable to various attacks and encounters. It is important to provide a secure and fast way for sharing these resources and avoid DOS/DDOS at the same time.

3. Existing Methodology and Drawbacks

Prevention using filters, Secure overlay, Honeypots, Load balancing are some existing measures to prevent DDOS attacks already existing in the field. These methodologies cannot be deployed in the Cloud environment because of some reasons mentioned below.

Firstly these methodologies can be also called multilayer DDOS prevention methodologies, most of these methodologies either block or trap the attackers based on various reasons, but when they do they do not give space for re - verification. Sometimes miscalculations may lead to the blocking of some unintended IP addresses. This may not be a big problem when it comes to non - service environments. But when it comes to service environments like cloud computing, quality of service matters and things have to be taken with great precautions so most of these methodologies are not used or used inefficiently.

3.1 Honeypots:

It's a sacrificial computer server that acts as a decoy to attract black hats. It creates a more attractive server that has high vulnerability inviting cyber - attacks. For instance, a honeypot might have ports that respond to a port scan or weak passwords. Vulnerable ports might be left open to entice attackers into the honeypot environment, rather than the more secure live network. Once the attacker enters the decoy website, the honeypot analyses the tools, tactics, and motives of the Black - hat.

Drawbacks:

1. Since the cloud is a public service platform, it is hard to target the attacker and so setting up a trap server using the honeypot technique will eventually affect standard users also.
2. In situations where the source of the attack is unknown, the honeypot technique becomes an inefficient methodology in cloud environments.

3.2 Load Balancing:

Load balancing is defined as the methodology of splitting workloads and computing properties in a server using a separate manager server. It enables an enterprise to manage workload demands or application demands by distributing the request load using separate servers. Load balancers add resiliency by rerouting live traffic from one server to another if a server falls prey to DDoS attacks or otherwise becomes unavailable.

Drawbacks:

1. On multiple server attacks, load balancing takes heavy processing time since it has to undergo three layers of service framework (Request Manager – Service Manager - Service Node).
2. Load balancing also fails to achieve SSL Offloading because it cannot handle encryption and decryption operations effectively.

4.3 Secure Overlay:

Many cloud users want more control over their data in motion, which is where overlay networks come in handy. Overlays are made up of a mesh of VPN connections that provide application owners with control over security, addressing, topology and protocol.

The Secure Overlay Service (SOS) architecture allows communication between a confirmed user and a target. A target is protected by removing all incoming packets from unapproved sources. A network that consists of the selected nodes forms an overlay that protects the specific target. All the packets are validated at entry points of the overlay and once inside are tunnelled securely to secretly designated nodes. Once the packets are validated, all traffic is forwarded to the target through the overlay network.

Drawbacks:

1. The multiple layers of software and processing provided by overlay networks can increase performance overhead and make the network more complicated.
2. The process of encapsulating and de - encapsulating packets can demand a significant amount of computing power.

4. Proposed system

The system architecture of the proposed system is as follows. The connection is passed to two intermediate servers called the Dam servers before the connection is directed to the cloud server. This Dam server is designed to carry out different protocols to find out for DDOS signatures and block them. Some of the processes that take place in the server are SPI, DPI, Recaptcha, Proxies and Load Balancing. SPI makes sure that forward proxy takes place with ease of complication. DPI verifies for traces of previous attacks in the metadata. Recaptcha and Proxies make sure that bots stay away from the system. Load balancing ensures that user - data interaction remains fast and bandwidth is conserved.

4.1. Architecture

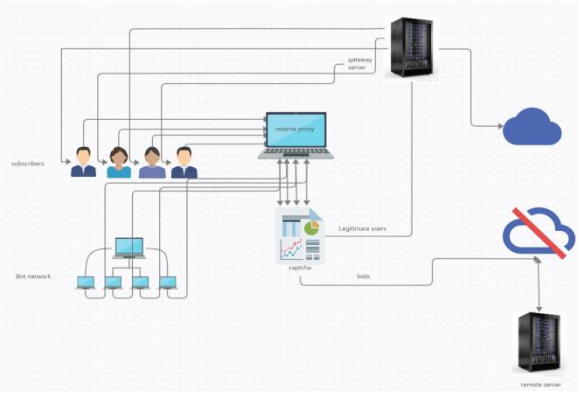


Figure 1: Architecture of the proposed system

4.2 System Overview

The proposed system has an increased security model to trash bots and improves the speed and security of the connection by transferring the legitimate connections from the “Dam one server” to a new gateway server called “Dam two server” so that traffic is controlled, basically acting as a load balancer and a firewall at the same time.

4.2.1. Dam one server

1. Shallow or Simple Packet Inspection tool

SPI separates destination and IP address from the incoming packet and sends it to the database on the second Dam server.

2. Forward proxy tool

Forward Proxy allocates a new proxy IP address from a list of predefined IP addresses to the public IP address from the user.

3. Recaptcha

Mouse movements can help identify bots by their pixelated or linear movements which are unusual from the random mouse movements from humans along with picture surveys that make it easy to evade bots.

4. IP check

IP check once again ensures that the received IP address is from our predefined allocated list.

4.2.2. Dam Two Server

1. Deep packet inspection tool

DPI tool evaluates the metadata and checks for signatures from previous attacks, blocks and trashes the request if found forged or suspicious.

2. Database

It serves as the database for the whole module.

5. Algorithm

Step A:

1. Extract IP address, destination address and port number using a simple packet inspection tool.

2. Forward proxy tool => send linking details to database => new IP

3. Forward request to recaptcha => verify user.

Step B:

1. Legitimate requests.

2. IF

IP address matches the IP range of proxy server forward connection.
ELSE
Drop connection and save request details in Database

Step C:

1. Transfer the request to Dam two server.

2. Deep packet inspection => check meta data

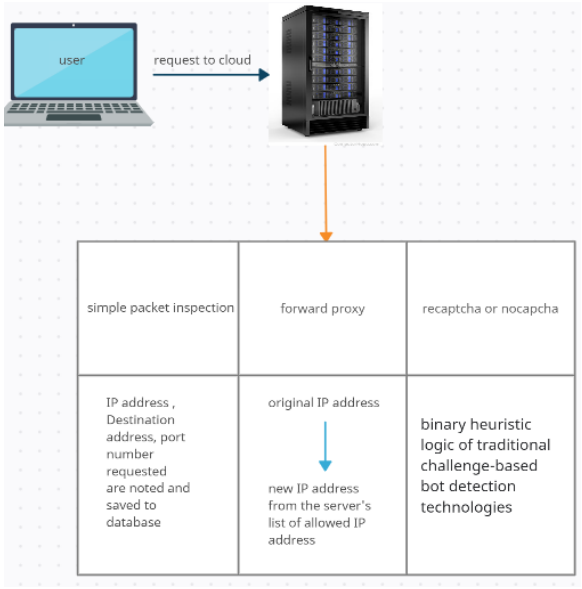
IF
Meta data matches signatures of attack
DO

2.1. Save all retrieved data =>
update database => alert

2.2. Drop connection
ELSE
Forward requested connection.

6. Methodology

- The clear representation of the packet from a receiver to the actual cloud server passes through these three important checkpoints before actually qualifying for access to the cloud server.



- The request packet is verified by the simple packet inspection tool and the derived details are stored in a database for future use.
- Then the Original IP address is covered with a proxy IP address, the proxy IP address is set from the allocated list of IP specified for the server so IP forgery attacks are eradicated.
- The request is then sent for captcha verification, where the user gets a prompt to verify if the request is made by a real human or computer.
- The user if successfully passes the captcha the request is then forwarded to the gateway server where reverse proxy takes place and the request is accomplished and stateful packet inspection is made.
- The stateful packet inspection takes a deep look into the metadata itself so that any unauthorised data request can be found and stopped before reaching the user.
- The data requested is then forwarded to the original IP to which the Proxy address points to.

7. Conclusion

Usage of forward proxy and reverse proxy saves bandwidth, response time and reduces the load on individual servers. Usage of Recaptcha gives protection from bots and computer - simulated requests. Gateway server acts as a load balancer. Data protection is facilitated because of the deep packet inspection; DPI will also look at the contents of a packet and check it against known patterns or signatures.

References

[1] Dhruba Kumar Bhattacharyya (2016), DDoS Attacks: Evolution, Detection, Prevention, Reaction, and Tolerance‖ ****
[2] "Understanding Denial - of - Service Attacks" US - CERT.6 February 2013. Retrieved 26 May 2016, Understanding Denial - of - Service Attacks | CISA ****
[3] Raghavan, S. V. (2011). An Investigation into the Detection and Mitigation of Denial of Service (DoS) Attacks, Springer ISBN 9788132202776 ****

[4] DOS Attacks - Rushikesh Gawande - DOS Attacks (ijsr. net) ****
[5] Protection of Server from Proxy - Based DDoS Attack - Poonam U. Patil, Dr. Y. V. Chavan - Protection of Server from Proxy - Based DDoS Attack (ijsr. net) ****
[6] G. Carl et al., Denial - of - amenity attack - detection techniques, IEEE Internet Comput., vol.10, no.1, pp.8289, Jan. /Feb.2006. ****
[7] "Using adaptive bandwidth allocation approach to defend ddos attack" - C H Lin, J C Liu, H CHuang and T C Yang - in MUE - pp.176 - 181, IEEE Computer Society, 2008. ****
[8] B. B. Gupta, R. C. Joshi and M. Misra - "Distributed denial of service prevention techniques" - CoRR, vol. abs/1208.3557, 2012. ****
[9] Detection And Mitigation of Distributed Denial of Service Attack by Signature based Intrusion Detection System - Hardik M. Shingala, Mukesh Sakle - Detection And Mitigation of Distributed Denial of Service Attack by Signature based Intrusion Detection System ****
[10] Algorithms for Packet Classification - Pankaj Gupta and Nick McKeown Computer Systems Laboratory, Stanford University - classification_tutorial_01.pdf (stanford. edu) ****
[11] A Survey of Denial - of - Service and Distributed Denial of Service Attacks and Defenses in Cloud Computing - Adrien Bonguet and Martine Bellaiche - https://www.mdpi.com/1999 - 5903/9/3/43/pdf ****
[12] Ramanpreet Kaur; Amrit Lal Sangal; Krishan Kumar - Secure Overlay Services (SOS) - A critical analysis 2012 II International IEEE Conference.
[13] Jaime Galán - Jiménez and Alfonso Gazo - Cervero - Overview and Challenges of Overlay Networks: A Survey | International Journal of Computer Science & Engineering Survey (IJCSES) Vol.2, No.1, Feb 2011.
[14] Using Cloud Computing to Implement a Security Overlay Network - Khaled Salah; Jose M. Alcaraz Calero; Sherali Zeadally; Sameera Al - Mulla; Mohammed Alzaabi; Published in: IEEE Security & Privacy.
[15] Mohammadreza Mesbahi; Amir Masoud Rahmani - Load Balancing in Cloud Computing: A State - of - the - Art Survey, I. J. Modern Education and Computer Science Published Online March 2016 in MECS.
[16] Pros and Cons of Load Balancing Algorithms for Cloud Computing - Bhushan Ghutke; Urmila Shrawankar | 2014 International Conference on Information Systems and Computer Networks.
[17] Cloud Security using Honeypot Systems - Nithin Chandra S. R, Madhuri T. M - International Journal of Scientific & Engineering Research Volume 3, Issue 3, March –2012.
[18] Honeypot: A Trap for Attackers - Savita Paliwal; International Journal of Advanced Research in Computer and Communication Engineering - Vol.6, Issue 3, March 2017.
[19] Security from various Intrusion Attacks using Honeypots in Cloud - Renu Meghani, Sanjay Sharma; International Journal of Emerging Technology and Advanced Engineering | Website: www.ijetae.com (ISSN 2250 - 2459, ISO 9001: 2008 Certified Journal, Volume 4, Issue 5, May 2014)
[20] Load Balancing Ranjan Kumar Mondal*, Payel Ray*, Debabrata Sarddar** International Journal of Research in Computer Applications & Information Technology Volume 4, Issue 1, January - February, 2016, pp.01 - 21ISSN Online: 2347 - 5099, Print: 2348 - 0009, DOA: 03012016 © IASTER 2016, www.iaster.com
[21] Lu, Yi, Qiaomin Xie, Gabriel Kliot, Alan Geller, James R. Larus, and Albert Greenberg. "JoinIdle - Queue: A Novel Load Balancing Algorithm for Dynamically Scalable Web Services. " Performance Evaluation 68, no.11 (2011): 1056 - 1071.
[22] Michael Armbrust, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy Katz, Andy Konwinski, Gunho Lee et al. "A View of Cloud Computing. " Communications of the ACM 53, No.4 (2010): 50 - 58.
[23] L. Spitzner. Honeypots: Tracking Hackers. Addison - Wesley Longman Publishing Co., Inc., Boston, MA, USA, 2002.
[24] Top 9 threats to cloud computing discovered by "cloud security of alliance" available at www.infoworld.com/article/2613560/cloudsecurity/9threats - to - cloud - computing - security.html.
[25] K. Santhi, "A Defense Mechanism to Protect Cloud Computing Against Distributed Denial of Service Attacks", "International Journal of Advanced Research in Computer Science and Software Engineering", Volume 3, Issue 5, May 2013.
[26] C. Duffy Marsan "Verisign to Extend Cloud - Based DDoS Protection to SMEs" Computer World K 10 May 2011

Author Profile

Nadesh. s pursuing B. E (CSE) from SRM Valliammai engineering college, Kancheepuram. My area of research includes Computer Networks and Network security.

Suriya K pursuing B. E (CSE) from SRM Valliammai engineering college, Kancheepuram. My area of research includes Cloud Computing and Network security**.**

Ashwin A pursuing B. E (CSE) from Rajalakshmi Institute of Technology, Chennai. My area of research includes Cloud Computing and Network Security.