International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2014): 5.611

An Efficient Way to Prevent Dos/DDos Attack in the Cloud Environment

Vaishali Hase[1], Harish Barapatre[2]

Department of Computer Engineering, Mumbai University, Y.T.I.E.T, Chandhai, Bhivpuriroad, Karjat

Professor, Department of Computer Engineering, Mumbai University, Y.T.I.E.T, Chandhai, Bhivpuriroad, Karjat

Abstract: ***In today, the most demanding service over the internet is cloud computing. Over the internet various packets are send and receives. At the time of sending and receiving packets various threats are encountered. One or more threats or attackers are involve in Distributed Denial of Service (DDoS). DDoS come into picture at the time of huge amount of packets are forwarded to a server from many computers. In the cloud computing there is various attacks like DOS (Denial of service) and DDOS (Distributed Denial of service). This paper proposed, attack can be overcome by Transmission Control Protocol (TCP) Mitigation Strategy which uses the SYN Cookie to prevent the attack in the cloud which the server ignores the connection packets when it receive the false or incorrect Acknowledgement (ACK) from the client which requested the connection. Proposed system gives the two layer of security.The server here has rules to be check whether it is a legitimate client or the spoofed one using the first layer of security for hop count filtering mechanism and second layer of security is encoding the sequence number of the SYN packet so that only a legitimate client can decode it. Additionally security is also provided for the data packets using the Message Authentication Code (MAC) and thus client is authenticated.***

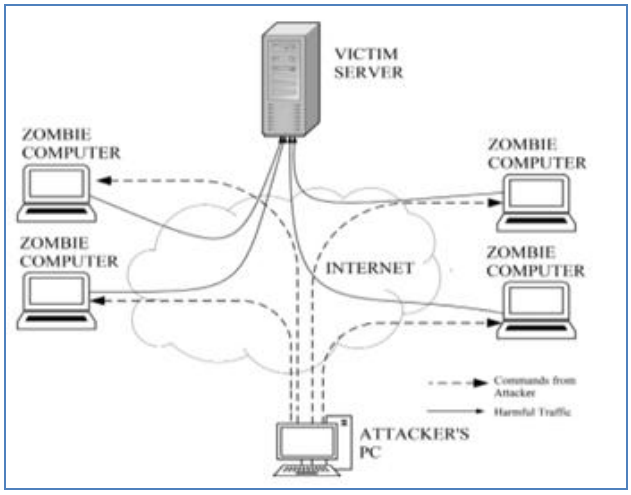
Keywords: Cloud computing, Virtualization, Denial of service DOS), Distributed Denial of service (DDOS), Filtering, Message Authentication code (MAC).

1. Introduction

Cloud computing is an evolving paradigm with various momentums, but its unique aspects security and privacy challenges. It explores the roadblocks and its solutions to providing a trustworthy cloud computing environment. Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort. Cloud computing has become a highly demanded service or utility due to the advantages of high computing power, cheap cost of services, high performance, scalability, accessibility as well as availability. Some cloud vendors are experiencing growth rates of 50% per annum. But due to being in a stage of infancy, it still has pitfalls that need proper attention to make cloud computing services more reliable and user friendly.

Sharing of resources over the cloud computing to achieve coherence and economies of scale similar to a utility over a network. Cloud computing is include broad concept of converged infrastructure and shared services in the cloud network which is used now in many of the IT organizations for efficient utilization of resources and to decrease cost of purchasing hardware infrastructures.

With many security challenges and vulnerabilities the technology VM is used in the cloud computing with new technology introduced in cloud computing it will take new number of challenges. New challenges addressed in the cloud computing that has experienced a drastic change in many organizations. Among various security and privacy have long term goal to be achieved in the cloud network. There has been significant research in this field, particularly on data leakage between running VMs and, in the case of public utility computing platforms such as cloud computing, the data leakage between a guest and the host itself is more vulnerable to different attack scenarios. The external attacks that attempt to directly target the VMs have been examined and it remains unclear whether virtualization is resistant to such attacks, or is even more vulnerable than conventional physical machines which are not virtualized. A denial-of-service (DoS) attack is characterized by an explicit attempt by the attackers to prevent legitimate users in the network from using those resources of the server. There are two general forms of DoS attacks in the cloud network: those that crash the various resources and those that flood different services in the environment.



DDOS attacks can be happen in many ways. One way is zombie computers or machines. As shown above figure attacker computers continuously flood the signals to zombie

computers. After that zombie computers schedules onset attacks on victim computers.

2. Literature Survey

Jin et al (2003) have proposed a novel filtering technique that is immediately deployable to weed out spoofed IP packets. Through analysis using network measurement data, they show that Hop-Count Filtering (HCF) can identify close to 90% of spoofed IP packets, and then discard them with little collateral damage. They implement and evaluate HCF in the Linux kernel, demonstrating its benefits using experimental measurements.IP spoofing has been exploited by Distributed Denial of Service (DDoS) attacks to (1) conceal flooding sources and localities in flooding traffic, and (2) coax legitimate hosts into becoming reflectors, redirecting and amplifying flooding traffic. Thus, the ability to filter spoofed IP packets near victims is essential to their own protection as well as to their avoidance of becoming involuntary DOS reflectors.

W. Eddy (2007) author describes TCP SYN flooding attacks, which have been well-known to the community for several years. Various Countermeasures against these attacks, and the trade-offs of each, are described. This author gives explanations of the attack and common defense techniques for the benefit of TCP implementers and administrators of TCP servers or networks, but does not make any standards-level recommendations.

Different counter measures against the SYN flooding attacks, and the trade-offs of each are described by W.Eddy (2007). In filtering method, author has proposed an efficient way to defence against the SYN flooding by the hop-count filtering method to differentiate the spoofed and the legitimate packets.

Mohd.Nazri Ismail et al (2011) has addressed in overcoming the problem in the attack detection stage using covariance matrix statistical method and attack source Time-To-Live (TTL) value counting method, the attack prevention will be based on Honeypot method and thus has efficiently overcome DOS and DDoS attacks in the cloud environment.

Padala P., Zhu X., Wang Z., Singhal S.,K. Shin., (2007), In this paper, they evaluate two representative virtualization technologies, Xen and OpenVZ, in various configurations. They consolidate one or more multi-tiered systems onto one or two nodes and drive the system with an auction workload called RUBiS. They compare both technologies with a base system in terms of application performance, resource consumption, scalability, low-level system metrics like cache misses, and virtualization-specific metrics like Domain-0 consumption in Xen.

3. Problem Statement

In the cloud computing the various packets are sends and receives over the internet. At the time of sharing resources and packets various attacks are encountered. So it is very important to provide a secured way for sharing resources and packets which prevents the DOS and DDOS attacks.

4. Mathematical Model

In a given system 'S'.

Input(I)= User request service to server.**Output(O)**= User get proper service.

Function=

- I*C*D=O

Control packet security(C)

- C= H*E

H=Hop count computation
E=Encoding and Decoding sequence numbers.

Data packet security (D)

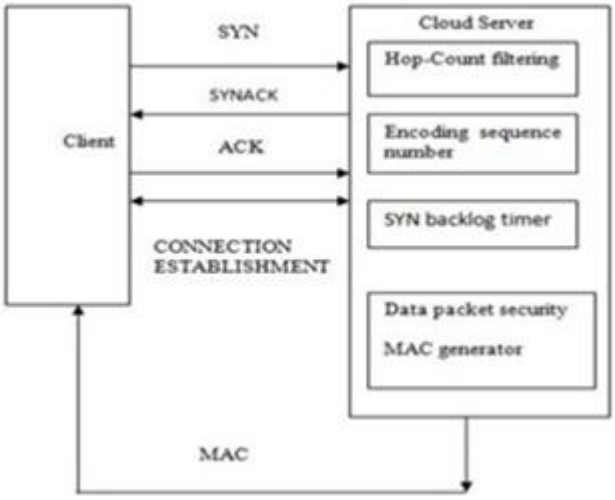
- MAC = C (K, M) (2)

K is the key (here, client IP and port number pair)
C is the code generated
M is the Message

5. Proposed System

A.System Architecture

System architecture of proposed system is as follows. According to below architecture this system performs the operations.



B.System Overview

Proposed system provides the two layer of security.

- The Control packet security.
- The Data security.

The Control packet security contains three phases.

- Hop-count computation and filtering of spoofed packets.
- Encoding and decoding the sequence number.
- Reducing SYN backlog timer.

The data packet security: The data packet security is obtained using the MAC Generator which distinguishes the packets that contain genuine source IP addresses from those that contain spoofed addresses in the network.

C.Algorithm and Technique

Control packet security:

It contains two algorithms.

- Hop count filtering:

Calculate hop-count (string SRCIP, Boolean SYN, integer finalTTL)
Hc = initialTTLfinalTTL
Hs = get stored hop-count value for the
IP address
If (Hc is not equal to Hs)

If (SYN _led is enabled)
Update the table with SRCIP, Hc
Else
It is a spoofed packet Drop the

Connection packet

Else
Encode the sequence number ( )

- Encoding and Decoding sequence number.

Encode sequence number ( )

1) Extract the SEQ number from the SYN packet
2) Encode the SEQ number using XTEA algorithm generate 32 bit encoded output
3) Send the 32 bit encoded value to the client in the SEQ number _eld of the SYN-ACK packet.
4) If it is a legitimate client, it decodes and sends ACK
5) If the server did not receive the ACK for the SYN received, it waits till SYN backlog timer expires, and drops the connection
6) Server establishes connection for the legitimate client
7) Else it is a spoofed packet, drop the connection packet

- Data packet security

If (connection == established)
Generate the MAC at server and send to
client
If (MAC at server = MAC at client)
Allow the packet to the server
Else
Drop the attack packet

The data is encrypted and appended along with the generated MAC using the MD5 algorithm. The client decrypts the data only it is s legitimate one and the MAC is generated for the decrypted data packet and the MAC is sent to the server as a piece of authentication.

6. Hardware and Software Requirements.

Hardware requirements.

- Intel core i3
- 2GB RAM
- 160GB hard disk drive.

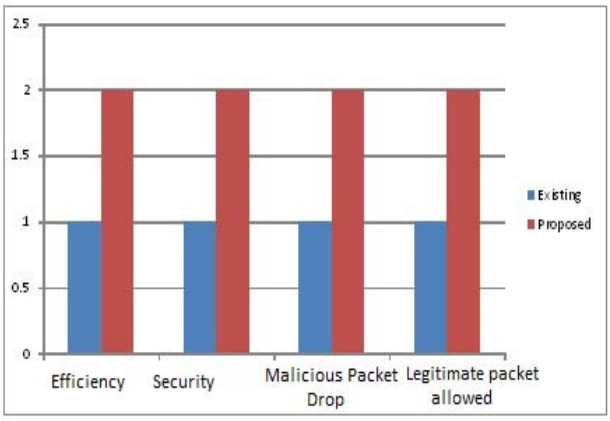
Software requirements.

- Windows 8 operating system
- Java net beans IDE 6.9
- Language used java (jdk 1.6).
- Cloud simulator 3.0.

7. Result and Analysis.

As shown in below graph the proposed system is more efficient than the existing system. The proposed system provides more security than existing system. Proposed system provides malicious packet drops function along with that it allow legitimate packet.

Proposed system provides to layer of security which enhance its performance than the existing system. Due to two layer of security only legitimate packet are transferred. And malicious packet gets dropped.



8. Acknowledgement

I would like to thanks all researchers for making their resources available. I would like to thanks to all the faculty members and Department of Computer Engineering Y.T.I.E.T, Bhivpuri road, Karjat, India for the guidance and cooperation.

9. Conclusion

In the cloud computing various packets are send and received at that time there is lots of chances that packet can be spoofed by attacker or attacker may block the service of authorized user. For that this paper proposed a new technic which allows an efficient way to prevent DOS that is denial of service and DDOS that is distributed denial of service over the internet. And also proposed system provides the two layer of security which enhanced the performance of proposed system along with that it provides more security and efficiency than existing system.

References

[1] Jin C., Wang H., Shin K., (2003), Hop-count filtering: An effective defence against spoofed ddos traffic, Proceedings of 10th ACM Conference on Computer Communication Security, pp. 30 41.

[2] Eddy W., (2006), Defences against tcpsyn flooding attacks, Cisco Internet Protocol Journal Vol. 8, Issue. 4, pp. 216.
[3] Padala P., Zhu X., Wang Z., Singhal S.,K. Shin., (2007), Performance evaluation of virtualization technologies for server consolidation, HP Labs Tec, pp. 1-14.
[4] Eddy W., (2007), RFC 4987: TCP SYN fooding attacks and common mitigations, pp. 19.
[5] A. Labrinidis and H. Jagadish, Challenges and Opportunities with Big Data, Proc. VLDB Endowment, vol. 5, no. 12, 2032-2033,2012.
[6] N. Venkatesu, et al., An Effective Defense Against Distributed Denial of Service in GRID, in Emerging Trends in Engineering and Technology ICETET '08., pp. 373-378.
[7] MohdNazri Ismail., AbdulazizAborujilah., Shahrulniza Musa., Amir Shahzad., (2011), New Framework to Detect and Prevent Denial of Service Attack in Cloud Computing Environment, International Journal of Computer Science and Security, Vol. 6, Issue.4, pp. 226-237.22

Author Profile

Mrs. Vaishali Hase is pursuing her M.E from Y.T.I.E.T college in Mumbai university. Before that she completed her B.E from Mumbai university. And her area of interest is Cloud computing.