ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 3, Issue 10, October 2016

Framework for Cloud Resilience System for Securing Cloud Infrastructure

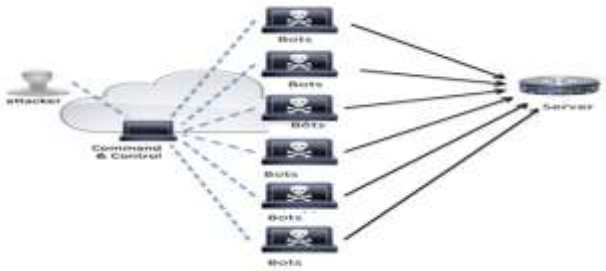
[1] Meera Gandhi [2] G. Aline Sophia
Sathyabama University
[1] meeragandhi.cse.sathyabama.ac.in [2] alinesophia.g11@gmail.com

Abstract:- **The main functionality of Cloud is to provide multiple resources to the users. Storing the data in the Cloud one of the major advantage. The hacker or the Bot master will try to access or try to gain information of the data which is stored in the Cloud, by sending multiple requests to the system. When the number of request exceeds the servers limit, the server will not be able to process the incoming request and the server may crash. The main aim of the paper is to create a framework for Cloud resilience system, which have the ability to provide the service for the clients even when the system is flooded with multiple request. When the incoming request exceeds the limit then the server will not be able to process the request and may crash. In order to prevent the server from crashing, a Stealthy DDos Detection Mechanism has been introduced. In this mechanism, the server monitors the number of incoming request given by each individual user. The server is initially given a limited amount of capacity to process the request of a single IP address. When the server load increases it checks all the request given by each user, if the request given by an individual user exceeds the servers limit then all the request from that particular IP address is blocked and all the services which are provided to that IP address is also denied.**

Key Words:-**Cloud resilience system, Stealthy DDoS detection, SIPDAS, Time based detection.**

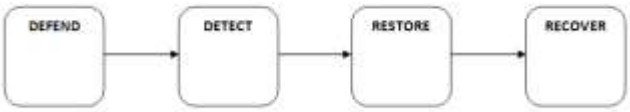
I. INTRODUCTION

In Cloud computing the Denial of Service (DoS) attack is an attempt to make the system resource or service unavailable for the intended users. The service is made unavailable by flooding the target system with enormous request so that the system is overloaded with traffic and prevents the legitimate user's request from not being fulfilled. The Distributed Denial of Service (DDoS) attack has become the major threat to computer networks. In DDoS attack, it requires multiple systems to attack the targeted system. The multiple systems are infected by Torjan which are called as botnets. These bots are programmed in such that they execute the command that has been given by the Botmaster or the attacker and run those command autonomously without the knowledge of the user. The major advantage of the attackers using the DDoS attack mechanism is that it has multiple system to generate traffic on the target system than using a single system machine.



II. METHODOLOGY FOR RESILENCE SYSTEM

The cloud resilience system, works in making the system function normally even after it has been distrupted. The process of the resilience system involves the method of defending, detecting, restoring and recovering. The system should be built in such a way that whenever a intruders tries to attack the system, the system should be able to overcome the attack. Once the attack has been initiated in the system, it should be able to detect the type of attack which has affected the system by the intruders. After detecting the malware, the system should restore the system and must overcome the malware.



ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 3, Issue 10, October 2016

III. CLOUD SERVER

The Cloud server holds a large amount of resources or services, the services may include image service, video service or a software service which depends on the request of individual users. The Cloud server enables the user to upload and download these services. When an individual is requesting for an image service, it will enable the user to view the image or to download the image from the Cloud server. When the request is for a video service, it will enable the user to view the video or to download the video from the Cloud server. When the request is for a particular software, then the software can be downloaded from the Cloud server.

IV. BOTMASTER APPLICATION

The Botnet is a number of interconnected network of computers that are affected with spyware without the knowledge of the user. These Botnets run autonomously on the targeted system and are controlled by the Botmaster, who initiate the command to each Botnets. The topology of Botnet is more resilient to shutdown, enumeration or discovery. Whenever the attacker calls the Botmaster the bots are created. The attacker waits until he gains enough bots under his control. Once the attacker gains the control of various bots, he starts to give command to the bots and these bots mindlessly executes the commands which are given to them. The DDoS detection mechanism is used to monitor the number of request given by each by each individual user. When the large number of request is from a single IP address for a particular time is considered to be the DDoS attack and the request from that particular IP address is blocked by the server.

V. SIPDAS ATTACK ALGORITHM

SIPDAS (Slowly Increasing Polymorphic DDoS Attack Strategy) algorithm is implemented by the attacker to perform the Stealthy DDoS attack. The term polymorphic represents the polymorphic attack, which change the message sequence at each mutation. Using SIPDAS, Botmaster performs attack to the Cloud through the bots. These bots will slow down the process of the Cloud, when this process increases the performance of the Cloud decreases and hence the server will not be able to respond to any client's request. In Stealthy SIPDAS Detection mechanism, the server maintains the record of the request given by every user. If the server load increases it checks each individual request of every user, if the request given by the user exceeds the server limit, the particular user IP address is blocked and the service is denied to that user.

VI. PARAMETER

- Integer CR ←I_0 {Initial attack intensity]
- Intensity (Interval between each submit) ← {Attack intensity increment}
- Threshold ← N_T(DOS attack threshold)
- Attack increment ← I
- Total Time (Total time the attack goes on) ←T {Burst period}

ALGORITHM

1. Repeat
2. t ← 0;
3. while t<=T do
4. nT← pick Random Tags (Threshold); compute Inter arrival Time(CR,nT);
5. tI ← compute Inter arrival Time(CR,nT);
6. send Message(nT,tI);
7. t ← t+t_I;
8. end while
9. if !(attack Successful) then
10. CR ← (CR +attack Increment); {Attack intensification}
11. else
12. while !(attack detected) and attack Successful do
13.{Service degradation achieved; attack intensity is fixed}
14. nT ← pick Random Tags(tagThresold);
15. Ti ← compute Inter arrival Time(CR;nT);
16. send Message(nT;tI);
17. end while
18. end if
19. tIM(CR)=compute Inter arrival Time(CR;NT);
20. tIm(CR) = compute Inter arrival Time(CR;1);
21. until (2/(tIM-tIm) < rate Threshold) and ! (attack detected)
22. if attack detected then
23. {Notify to the Master that the attack has been detected}
24. print "Attack detected";
25. else

VII. TIME BASED DETECTION

The time based detection algorithm will help to detect the malware in the cloud system. The malware is detected by recording the number of request given by the

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 3, Issue 10, October 2016

each user for a limited time. The time limit is fixed depending on the server capacity. Let us consider that, for a particular time‘t’ the number of request from a single IP address should not exceed the threshold value.

ALGORITHM

Get the request from the user
    Set the threshold value based on the request
If req > threshold value then
    Block the IP
End

VIII. HEAP SPACE MONITORING

Each user is allocated with the memory space based on their IP address. The entire request given by each user are stored in their memory. When the space in their memory gets filled, then the request from that particular IP address is blocked. Inoder to maintain the servers performance. Once the request are prossessed and the memory space is free, then the request from that IP address is resumed.

IX. CONCLUSION:

In the internet, there are huge number of attackers, who implement the DDoS attack on the system, which causes a serious threat to internet and web applications. The main aim of this paper is to avoid the server crash that is preventing the system resources being unavailable. The Slowly Increasing Polymorphic DDoS attack is detected using Heap Space Monitoring.

REFERENCES

1.Massimo Ficco and Massimiliano Rak,”Stealthy Denial of Service Strategy in Cloud Computing”-IEEE Tranactions on Cloud Computing, vol. 3, no. 1, Jan-Mar.2015.

2. C. Mont, K. McCorry, N. Papanikolaou, and S. Pearson,”Security and Privacy Governance in Cloud Computing via SLAs and a Policy Orchestration Service”- 2 nd International Conference on Cloud Computing and Services Science, 2012, pp. 670-674.

3. Ms. Parag K. Shelke, Ms. Sneha Sontakke, Dr. A. D. Gawande, “Intrusion Detection system for Cloud Computing”- International Journal of Scientific & Technology Research, vol. 1, Issue 4, May 2012.

4. Y. Zhang, Z. M. Mao, and J. Wang, “Low-rate TCPtargeted DoS attack disrupts internet routing,” - 14th Network Distributed Systems Security Symptoms, Feb. 2007, pp. 1–15.

5. K. Lu, D. Wu, J. Fan, S. Todorovic, and A. Nucci, “Robust and efficient detection of DDoS attacks for largescale internet”-In Computer Networks, vol. 51, no. 18, 2007, pp. 5036-5056.

6. H. Sun, John C. S. Lui, and D. K. Yau,”Defending against low-rate tcp attacks: Dynamic detection and protection”- 12th IEEE International Conference on Network Protocols, 2004, pp. 196-205.

7. Kuzmanovic and E. W. Knightly,” Low-rate TCPTargeted denial of service attacks: the shrew vs. the mice and elephants”- International Conference on Applications, technologies, architectures, and protocols for computer communications, 2003, pp.75-86.

8. M. Guirguis, A. Bestavros, I. Matta, and Y. Zhang,“Reduction of Quality (RoQ) attacks on Internet End-Systems”- IEEE International Conference on Computer Communications (INFOCOM), pp. 1362-1372, Mar. 2005.

9. Xiaodong Xu, Xiao Guo, and Shirui Zhu,“A queuing analysis for low-rate DoS attacks against application servers”- IEEE International Conference on Wireless Communications, Networking and Information Security, 2010,pp. 500-504.

10. Lanjia Wang, Zhichun Li, Yan Chen, Zhi Fu, Xing Li,“Thwarting Zero- Day Polymorphic Worms With Network-Level Length-Based Signature Generation.”- IEEE/ACM Transactions on Networking, 2010, pp. 53-66.

11. Chonka, Y. Xiang, W. Zhou, and A. Bonti, ”Cloud security defense to protect Cloud computing against HTTP-DOS and XML-DoS attacks”- In Journal of Network and Computer Applications, vol. 34, no. 4, July 2011, pp. 1097-1107.

12. S. Ebrahimi-Taghizadeh, A. Helmy, and S. Gupta, “TCP vs. TCP: A systematic study of adverse impact of shortlived TCP flows onlong lived TCP flows,” - IEEE

International Conference on Computer Communications, Mar. 2005, pp. 926–937.

13. M. Guirguis, A. Bestavros, I. Matta, and Y. Zhang, "Reduction of quality (RoQ) attacks on dynamic load balancers: Vulnerabilityassessment and design tradeoffs," IEEE International conference on Computer Communications, 2007, pp. 857–865.

14. Y. Xuan, I. Shin, M. T. Thai, and T. Znati, "Detecting applicationdenial-of-service attacks: A group-testingbased approach,"IEEE Transient Parallel Distributed Systems, vol. 21, no. 8, pp. 1203–1216, Aug. 2010.

15. V. Durcekova, L. Schwartz, and N. Shahmehri, "Sophisticateddenial of service attacks aimed at application layer," - 9 thInternational Conference ELEKTRO, 2012, pp. 55–60.

16. U.Ben-Porat, A. Bremler-Barr, and H. Levy, "Evaluating the vulnerabilityof network mechanisms to sophisticated DDoS attacks,"-IEEE Inernational Conference on Computer Communications, 2008, pp. 2297–2305. International Conference on Current Research in Engineering Science and Technology (ICCREST-2016) E-ISSN :2348 – 8387 www.internationaljournalssrg.org Page 42

17. Y. Chen and K. Hwang, "Collaborative detection and filtering of shrew DDoS attacks using spectral analysis," - J. Parallel Distributed Computer, vol. 66, no. 9, pp. 1137–1151, Sep. 2006.