IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-7, Issue-3, March 2019 E-ISSN: 2347-2693

Alleviation of DDOS Attacks to Achieve Data Asylum In Cloud Computing

Ashok Koujalagi

Dept. of Computer Science, Basaveshwar Science College, Bagalkot Rani Channamma University, Karnataka, INDIA

Corresponding author: koujalagi.ashok@gmail.com

DOI: https://doi.org/10.26438/ijcse/v7i3.972975 | Available online at: www.ijcseonline.org

Accepted: 17/Mar/2019, Published: 31/Mar/2019

Abstract: Data Security and privacy become the critical issue as cloud computing is getting famous for web-based services in modern era. Because cloud computing is providing Data access to everyone, data security become critical issue that limit many cloud based applications. Major issue of security in cloud computing because users can access sensitive data. One of these security challenges in cloud computing, Distributed Denial of Service (DDOS) attack is the major security threat to Web-applications as well as cloud computing. Attackers try to compromise the security with heavy traffic from different resources. This research will observe the effects of Distributed Denial of Service (DDOS) attacks on cloud server moreover mitigation technique will be discussed to prevent DDOS attacks on the cloud.

***Keywords*:** Cloud Computing, Data Security and privacy, Data mitigation technique, DDOS

I. INTRODUCTION

Cloud computing are Extremists generally popular in recent years because they offer powerful systems for users on the Internet. The main cloud is the speed and reliability. Many forums come to traditional glasses, so Small can create clones several times; although the daily consumer tool is in the cloud, the source is very dangerous. But trust, privacy and security become the major concern as more people and organization start using cloud computing. Some experts suggest putting security on priority before implementing cloud services to ensure the protection of user's data. Most of cloud service providers giving different type of storage services that offer large cloud based space for users like Dropbox, Amazon, Gdrive and MS OneDrive. Because of its nature of service clouds can give services to users with malicious purpose and hackers can use these services in malicious way like hosting a malicious application on a cloud server to arrange a DDOS attack on any other server or on its own host.

DDOS attack is a combine task done by multiple infected computers on availability of a single particular victim system. Because of basic characteristics of resources in cloud at network, host and application level, it's easy for attackers to do DDOS attacks. DDOS attacks are major challenge for clouds which can cause billions of dollar loss. There are other solutions to handle the security issues as cloud infrastructure in internet environment but some security issues exist especially in cloud because of the nature of cloud environment.

DDOS is an actual challenge to availability in cloud computing. By flood traffic generated by botnet, DDOS attack prevent user to avail services offered by cloud providers and use bandwidth as much as possible to crash the servers. Spoofing of IPs is a main term of DDOS attacks. It helps to hide the real identity of hacker or attacker from victim. As result detection of DDOS attack takes more time and resources.

Clouds have three major aspects which are confidentiality, availability and integrity and DDOS attacks are directly effect on availability of clouds. On other side there are also several ways to handle popular security threats on internet which may be useful for cloud computing but most of them need more improvements to work efficiently with cloud computing. Security for DDOS attacks in cloud computing and protection against DDOS attacks in cloud computing will be discussed. In entire research, problem and the solution about DDOS attacks on cloud will be discussed briefly.

INFORMATION RETRIEVAL

The present study focuses on the 'Distributed Denial of service attacks.' The research will highlight the details about the DDOS attacks and define a comprehensive framework for the DDoS protection.

To begin with, let us understand the basic working and information about the DDoS attacks which will be helpful in comprehending the problems faced by web servers appropriately. Lately, almost every vendor is using online store for the development and enhancement of their business

© 2019, IJCSE All Rights Reserved

in the industry. The trend has become famous largely due to time restraints and customers prefer the portable ease of access and the reliability factors during their purchases. Therefore, the information about the products is readily available on the online web servers. In this scenario the hitch occurs when the server stops working leaving the vendor at loss as to what the issue is.

Figure 1: Cloud Computing Architecture

Amid occasions once the online server abruptly quits operating with none warning signal, it means the Fake traffic is disturbing the site and subsequently the server is facing downtime that is actually a DDoS attack.

SECURITY DESIGN

Broad analyzes and reviews focus on the strategy of structural safety requirements and to determine the safety requirements. To have the ability to agree with the definitions used to characterize 'acronym, definitions and domain-specific information'; installed by all invested individuals. It may be worth checking and specifying certain security requirements of the invited individual. Has the ability to define security goals that lead to a clear definition of what is expected of the security guard, strategies, and business framework. This concrete recommends that the creation of artifacts for events occurs, similar to cases of abuse and templates for specifications and structures. To conduct a risk assessment that can facilitate risk analysis for all known security goals that lead to threat analysis. To select acquisition techniques that also includes system identification and analysis of the protection requirements of all stakeholders. This is often done through interviews, process modeling and business simulations, prototypes, discussions and focus teams. This section includes the introduction of security level, cost-benefit analysis, structural culture, structure and greatness.

DDOS ATTACK TAXONOMY

There is no intensive information available or research conducted to develop taxonomy for DDoS attacks within the cloud with special emphasis on information measure attacks and depletion of resources. However, DDoS attacks targeting web services within the cloud are classified into massive payload, powerful analysis and flood attacks, whereas DDoS attacks are categorized into infrastructure levels.

Attacks the current study classify DDoS attacks in application-level attacks and infrastructure level attacks. it's been argued that classification supported a stratified structure are going to be helpful to alter the attack method for readers – see Figure 2

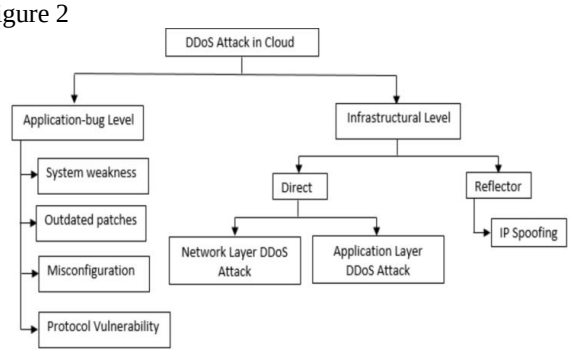

Figure 2: DDoS attack taxonomy in cloud

APPLICATION-BUG LEVEL DDOS

To carry out attacks at the level of application error, hackers take full advantage of the weaknesses found in the system, which creates inconveniences in the cloud resources for users. Some common attack vectors are: protocol vulnerability, system weakness, patches exceeded and incorrect configuration. For example, the weaknesses found in the protocol of that area unit used by the target applications can be used by the attackers through a method that involves causing specially designed packages to overload the application; it's crashing.

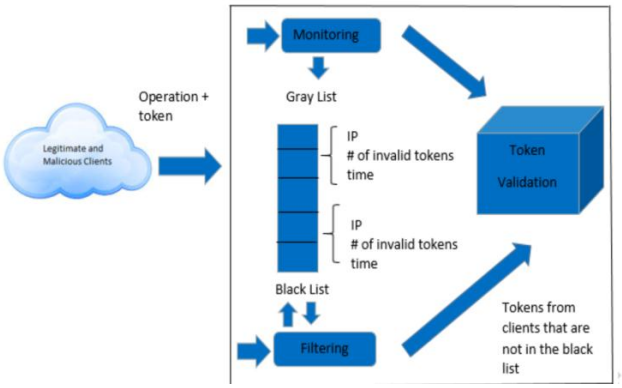

Figure 3: Client Control Solution Architecture

II. PROCEDURE

Check based interruption location endeavors to characterize an arrangement of standards (or marks) that can be utilized to choose that a given plan is that of a gatecrasher. Therefore, signature based frameworks are fit for accomplishing large amounts of exactness and negligible number off lagers encouraging points in recognize in interruptions. Little variety in known assaults May likewise influence the

© 2019, IJCSE All Rights Reserved

examination is if a discovery structure isn't legitimately arranged. Thusly, signature based identification neglects to distinguish obscure assaults or assortment of known assaults. One of the rousing motivations to use signature based identification is ease in keeping up and refreshing preconfigured rules. These marks are formed by a few parts that perceive the movement. In Cloud, signature based interruption recognition system can be used to identify known assault with detection of attackers IPs. It utilized either at front-end of Cloud to identify outside interruptions or at back end of Cloud to perceive external/inward interruptions. Mark based intrusion area system for perceiving interferences on VMs (or front end of Cloud condition) and IP detection based on stopforumspam API identify known attackers IPs and run-time prevention happened after insertion in database table – see Fig 4.

DDOS Attacks generated by botnet on Web-Application hosted on cloud. AWS (EC2) has been used for Cloud environment. Attacks simulated in DDOSIM.Ips of zombie systems detected with the help of API and blocked on run-time. To protect cloud not only with simple method of IDS detection of analyzing the signature of data packets and prevent it viewing the all critical traffic on network.

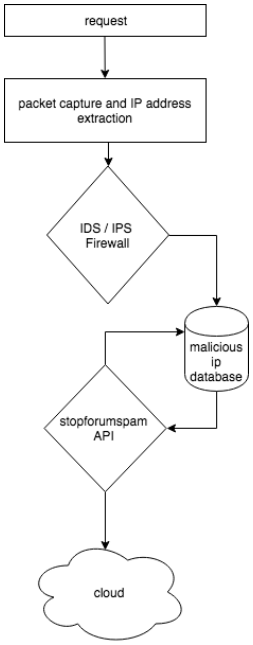

Figure 4: stop forum spam API including IDS/IPS to secure Cloud Computing.

III. FEATURE EXTRACTION

The system of highlight extraction separated the whole bundles and ascertains the usefulness of every datum parcel which influenced the server either the bundle is genuine or contaminated. These highlights helped in introductory discovery of the bundle and forward that parcels to the motor where the improvement of the parcel can be tried now the inquiry emerges about the relationship motor. The component extraction broke down the parcels in light of their:

- Normal Packet Size
- Variance in time interval
- Rate of per bits

These above highlights helped us for the location of the tainted movement which can down the site for the long interim of time. Some past arrangements helped us in the combination of the new assurance administrations.

Gridlock Aggregation; catch the parcel and forward that bundle to the particular hub which wanted by the system with the goal that it could be simple for us to distinguish the tainted IP deliver as indicated by their source and the goals.

Table 1: Aggregation of Traffic

Proposed system evaluation results	**False Alarm**		**Correct detection**	
	Normal Data (False Positive Rate)	***Attack Data (False Negetive Rate)***	***Normal data (True Negetive Rate)***	***Attack Data (Ture Positive Rate)***
UCLA DATASET	0.01	0.02	0.98	0.97
Simulated Network	0.03	0.04	0.96	0.96

IV. CONCLUSION

The DDoS attack presents real-world problems and tests the extent of its development and recognition by the entire population, government organizations and suspects. In this dissertation, I try to reach a reasonable perspective on the issue of DDoS attacks and various proposed resistance constraints. With a clear perspective on this problem, our reasoning has been relieved and in this sense we can find a more convincing answer regarding DDoS attacks. One of the privileged positions for raising the attack system and protecting against DDoS attacks is that correspondence and collaboration between experts can be achieved to differentiate the gap in the DDoS field. This classification must be continuously updated, as new hazards and protection components are detected. Their incentive to pursue research and exchange is undoubtedly broad.

REFERENCES

[1]. Balobaid. A, Alawad. W and Aljasim. H. 2016. Study on the impact of DoS and DDoS attacks on cloud and mitigation techniques. 2016 International Conference on Computer, Analytical and Security Trends (CAST), Pune, India, 1 (1): 416-421.

[2]. Changes. V and Ramachandran. M 2016. Towards the acquisition of data security with the cloud computing framework. IEEE transactions on a service computer, 9 (1): 138-151.

© 2019, IJCSE All Rights Reserved

[3]. Li. Y, Gai. K., Qiu. L., Qiu. M and Zhao. H. 2017. Intelligent cryptographic approaches to deploy large data storage in cloud computers. Information Science, 387 (1): 103-115.
[4]. Manogaran. G, Thota. C and Kumar. M 2016. MetaCloudDataStorage Architecture for Great Data Security in Cloud Computing. Computer Science Procedures, 87 (1): 128-133.
[5]. Osanaiye. Oh, Choo. R, and Dlodlo M. 2016. Distributed Discontinuing Service (DDoS) in the Cloud: Cloud Vision Overview and DDoS Mitigation Framework. Computer Networks and Applications Journal, 67 (1): 147-165.
[6]. Osanaiye. O. 2015. Title: IP Spoofing Detection to Prevent DDoS Attacks in Cloud Computing. 2015 International Conference on Intelligence in Next Generation Network, Paris, 1 (1): 139-141.
[7]. Sabahi. F., 2011. Threats and cloud computer security responses. IEEE International Conference on Software and Communications Network, Xi'an, 1 (1): 245-249.
[8]. Sow. A, Earring. R and Radzik. T. 2016. Detection of known and unknown DDoS attacks via artificial neural networks. Neurocomputing, 172 (1): 385-393.
[9]. Shameli-Sendi. A, Pourzandi. M, Fekih-Ahmed. M and Cheriet. M. 2015. The reduced taxonomy of Denial of Service Blocking brings closer to the cloud computer. Computer Networks and Applications Journal, 58 (1): 165-179.
[10]. Somani. G, Gaur. M, Sanghi. D, Conti. M and Buyya. R. 2017. Resizing services for fast DDoS reduction in cloud computing environments. Annale van Telecommunicatie, 72 (5): 237-252.
[11]. Thapngam. T, Yu. S, Zhou. W and Makki. S. 2014. Service Disclaimer Tracking (DDoS) is exposed by traffic pattern analysis. Peer-to-peer Networks and Applications, 7 (4): 346-358.
[12]. Xiao. P, Li. Z, Qi. H, Qu. W and Yu. H. 2016. DDoS Detection Effective With Bloom Filter In SDN. 2016 IEEE Trustcom / BigDataSE / ISPA, Tianjin, China, 1 (1): 1-6.
[13]. Yu. S, Tian. Y, Guo. S and Wu. D. 2014. Can we defeat DDoS attacks in the cloud? IEEE transactions on parallel and distributed systems, 25 (9): 2245-2254.
[14]. Yang. L, Zhang. T, Song. J, Wang. J and Chen. P. 2012. DDoS attack defense for cloud computers. 2012 International Conference on Computer Science and Automation Engineering (CSAE), Zhangjiajie, China, 1 (1): 626-629.

About the Author

Dr. Ashok Koujalagi is an Author, Professor and Postdoctoral Researcher. He received his M.Sc degree from Bangalore Central University. And Ph.D from Central University of Allahabad. He authored four books among one is International, he also has more than 24 research publications & Proceedings indexed in ICI, Scopus, SCI, Copernicus, WoS.
Presently serving as an Assistant Professor & Postdoctoral Researcher in the Post Graduation Department of Computer Science, Basaveshwar Science College - Bagalkot, affiliated to Rani Channamma University - Belgaum, Karnataka, INDIA.
He is also Professional Board member of 21 International Organizations / Association, Editorial Board Member in 13 International Journals, Peer-Reviewal Board Member in 15 International Journals and Advisory Board Member in 3 International Journals. He has also been invited by 4 international conferences as a "Conference Organizing Committee Member, also invited as a speaker in 6 international Conferences. And his area of research covers, Computer Networking, Cloud Computing, Data Mining, and Mobile Computing.

© 2019, IJCSE All Rights Reserved