International Journal of Grid Distribution Computing
Vol. 8, No. 3, (2015), pp.119-126
http://dx.doi.org/10.14257/ijgdc.2015.8.3.12

Comprehensive Study of Various Techniques for Detecting DDoS Attacks in Cloud Environment

Navdeep Singh, Abhinav Hans, Kapil Kumar and Mohit Pal Singh Birdi

M. Tech Computer Science
Department of Computer Science
GNDU Regional Campus Jalandhar
Navvdeep.singh@gmail.com

Abstract

Cloud computing is the most dynamic field of IT industry. It is becoming very famous due to its less resource consuming and higher output. Though Cloud computing is very vast and useful technology but it is not remained untouched from attackers or hackers. The most common attack notified on the cloud environment is DDoS attack. DDoS attacks i.e. Distributed Denial of service attacks happens on a cloud environment in such a way that, two or more than two attackers sends the multiple SOAP requests at the same cloud server and consume all the legitimate resources. From the study it has been concluded that, none a system is developed so far to prevent the DDoS attacks completely because even the detection of DDoS attacks is a major issue and prevention is a very big thing to achieve after detection and mitigation. This paper is focused on underlying the introduction about DDoS attacks and the next part of the paper is followed by the comparative analysis of the different techniques and algorithms used in detecting the DDoS attacks in cloud environment.

Keywords: *Distributed Denial of Service, Cloud Computing, Web Services*

1. Introduction

The technology demanding less resources and with supreme output always attracts the user. So the Cloud Computing is the one which provides the same and entices the users. The cloud system provides a distributed system over a network on which more than one computer or mobile phones connected on the same time. Cloud computing can also be considered as the allegory of internet. Cloud service providers must certain about that they get the security flanks [1]right; they are the one which take the responsibility if the things went wrong in the cloud system. Cloud computing provides many benefits like fast deployment, software rental service, lesser cost, less hardware cost, scalability, elasticity ,low cost recovery and data storage solutions, on-demand security controls, real time detection of system tampering and rapid re-constitution of services.

The most highlighted feature of the cloud system is the rental service *i.e.* if the user does not have the particular software then the user can use that software on the cloud and can pay for it. Obviously if the user wants to buy his own software then the hardware and software cost will be counted. So it will be better to use the cloud system instead. The cloud system consists of three types of delivery models based on the resource focus *i.e.*, SaaS, PaaS and IaaS. Saas stands for software as a service that grants end users to use cloud applications [2]. In the SaaS the data resides on the outer boundaries of the enterprise. The Google application store is the best example of the SaaS. The next delivery model PaaS stands for Platform as aService in which developer can develop applications using the programming languages and tools supplied by the cloud provider. And the last service model Infrastructure as a Service (IaaS) allows user to quickly regulate the physical resources for the applications and run any software ranging from

ISSN: 2005-4262 IJGDC

operating systems to application software [3]. Amazon and Amazon S3 are the best known examples.

But whenever a developer designs any sort of hardware or software the first thing that took into consideration is that how secure the software or hardware is. Security is the main part [4] of the any system [4]. Though the cloud offers the spectacular advantages but there are also some security issues yet to be solved. Among the security issues the Denial of service is most considerable and most happening threat in the cloud computing.

Denial of service attacks is one of the major threats on the emerging technology. Denial of service attacks aims at the using all the resources by sending fake requests in very large amount and the threat is that these requests are difficult to detect.

The Dos attack also is considered when the odd messages attack the all nodes by different nodes at the same time [5]. This type of attack is called distributed denial of services (DDoS). DDoS (Distributed Denial of Service) attacks are the most highlighted factor amid network security risks in cloud server [6]. DDos attack undertakes the all resources with sending fake requests and a machine or network resource unavailable to its intended users. Although the means to carry out, motives for, and targets of a DoS attack may vary, it generally consists of efforts to temporarily or indefinitely interrupt or suspend services [7].

IT sector is the most booming sector and according to many surveys most of the DDoS attacks took place on IT sectors. In this area, many private companies owned their own cloud servers. Cloud server is the main target of the attackers now days because it contains a lot of data. The number of such DDoS incidents [8] is consistently increasing. For example, the figure [9] is showing the DDoS attacks in various sectors. Most of the attacks have been reported in the IT field.

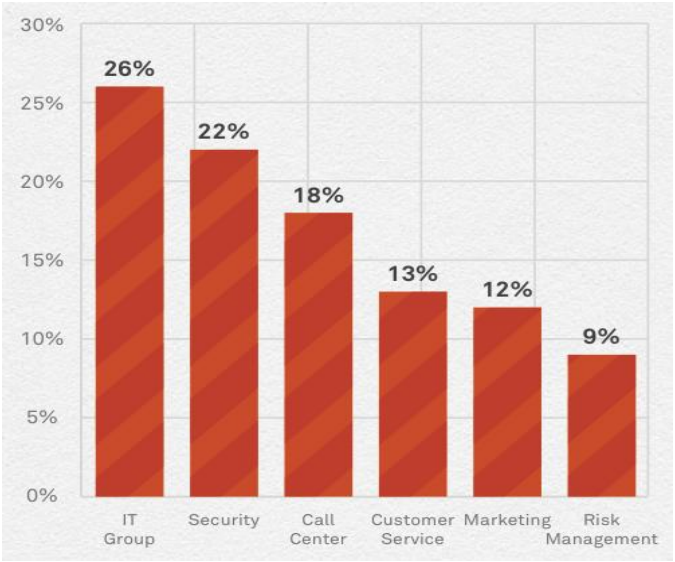


Figure 1. DDoS Attacks in Various Technologies

This paper is focussed on reviewing the various techniques or algorithms designed to detect the DDoS attacks in the cloud environment.

2. Comparative Parameters

2.1. Throughput

Throughput is the amount work that computer can do in a given period of time. It is a measure of comparative effectiveness of large computers that run programs concurrently.

2.2. Fault Tolerance

Whenever an unexpected fault or error arises in the system that property which prevents the system to go in failure or crash state and let the system to continue its work is known as fault tolerance.

2.3. Performance

Performance is denoted by the amount of useful work accomplished by a computer system or computer network compared to the time and resources used. Depending on the context efficient performance depends on the shortest response time, high throughput, low utilization of computing resources, high availability *etc*.

2.3. Overheads

Overheads are any combination of excess or indirect computation time, bandwidth, .memory or other resources that are required to attain a particular goal.

2.5. Response Time

The amount of time between a single interactive user requests being entered and receiving the application's response is known as response time

3. Existing Techniques for Detecting DDoS Attacks

In this section, we present a summary of existing literature on DDoS attack detection methods. These methods are based on the architectures discussed above namely, victim-end, source-end and in-network. We discuss these schemes without considering their practical deploys ability in real networks. Recent trends show that soft computing approaches have been used heavily for DDoS attack detection.

3.1. Statistical Methods

Detection of DDoS attacks can be done by exploiting statistical properties of normal requests and patterns of attack. In [10] a statistical model is explained in which a statistical model for normal traffic is fitted and then a statistical inference test is applied to determine if a new instance belongs to this model. Instances that do not conform to the learnt model, based on the applied test statistics, are classified as anomalies. In [11] distributed change point (DCP) detection architecture is used along with change aggregation trees (CATs) and non-parametric CUSUM (cumulative sum control chart). When a DDoS flooding attack is being launched, the cumulative deviation is noticeably higher than random fluctuations.

3.2. Intrusion Detection System

The Most standard feature of IDS is that it reliable for each virtual machine in cloud environment. This is the method is used for detecting the DDoS attacks in [12]. In IDS system, the IDS is used at the cluster controller. And it is applied to each virtual machine and in this way cloud computing platform avoids the overloading problem that could be caused by DDoS attack. And further more advantage of this strategy as described by Roschke, *et. al.* (2009) is the benefit of reducing the impact of the possible attacks by the IDS Sensor VMs.

3.3. IDS Based DempsterShafer Theory

This technique is mainly focuses on detecting and analyzing the Distributed Denial of Service (DDoS) attacks in cloud computing environments. The DDoS attacks mainly

targets on cloud service disruptions. In [13] a solution is imposed to combine the previous work of Intrusion Detection Systems (IDSs) deployed in the virtual machines of the cloud environment along with a data fusion methodology in the front-end. So when the attacker attacks cloud system, the VM-based IDS will get a warning, which will be stored into the Mysql database or any database that is joined to the cloud system placed within the (CFU) *i.e.* Cloud Fusion Unit of the front-end server. A quantitative solution is proposed for analyzing alerts generated by the IDSs, using the Dempster-Shafer theory (DST) operations in 3-valued logic and the fault-tree analysis (FTA) for the mentioned flooding attacks. At the last step, solution uses the Dempsters combination rule to fuse evidence from multiple independent sources.

3.4. Packet Information Gathering and Pre-processing

DDos attacks have many categories like Zobbie Cloud Client, related to virtual machines a like hypervisor attack of virtual machine. In [14] authors concentrated on detecting the hypervisor attack. When this attack took place it causes the resource imbalance and data loss. The detection procedure is done with packet analysis that consist a packet loader and packet collector. Packet loader stores the files about collected packets using packet capture tool in HDFS. Packet collector performs packet information gathering through Libcap and Jpcap module from live interface.

3.5. Host Based Intrusion Detection Systems

In [15] author explained a host based intrusion detection system *i.e.* HIDS which monitors and analyzes the information collected from a host machine. And the detection procedure follows in which the different type of the information such as system files used, calls of system, type of data etc. Then this detection system observes the modification in the host kernel and also checks for program's behaviour. If any deviation is observed from the default behaviour then the report of the attack is generated.

3.6. Network Based Detection System

In [16] author proposed network detection solution by combining supervised learning technique and unsupervised learning technique. They used K-Means algorithm for unsupervised learning and Naive Bayes algorithm for supervised learning. The first step of algorithm is using K-Means algorithm to group data to normal or attack. Then, use Naïve Bayes algorithm to classify the obtained result into attack type. The KDD99 dataset was used to evaluate the performance of this algorithm. The detection rate was improved to 99.6 percent. However, this solution is not practical for real network because K-Means algorithm requires more time to process huge data in real networks which could lead to bottleneck problem and system clash.

3.7. Real-Time Detection System

In [17] authors proposed a real-time detection approach. They used packet sniffer to sniff network packets in every 2 seconds and pre-processed it into 12 features and used decision tree algorithm to classify the network data. The output can be categorized into 3 types which are DDoS, Probe and normal. The result shows that this algorithm as 97.5 percent of detection rate. This technique is fast and able to use in real network. However, it was not designed to detect unknown attacks.

Though there are many techniques are developed so far to detect and mitigate the DDoS attacks in the cloud environment but none a perfect technique has been developed yet. In this paper different types of the technologies have been discussed and the comparison is done on the basis of different parameters. The table below shows the

different parameters of different techniques that have been taken from the previous studies and works and a comparative analysis is done on the basis of same.

Table 1. Comparative Analysis of Different DDoS Detection Techniques

Name of Techniques	Throughput	Fault Tolerance	Performance	Overheads	Response Time	Detection Rate (%)
STATISTICAL METHOD	NO	NO	YES	NO	NO	NA
IDS	YES	NO	YES	YES	YES	NA
IDS BASED DEMPSTER-SHAFER THEORY	NO	YES	YES	NO	NO	NA
PACKET INFORMATION GATHERING AND PRE-PROCESSING	NO	NO	NO	NO	NO	NA
HOST BASED INTRUSION DETECTION SYSTEMS	NO	NO	YES	NO	YES	NA
NETWORK DETECTION SYSTEM	NO	YES	NO	NO	NO	99.6
REAL-TIME DETECTION SYSTEM	YES	NO	YES	YES	YES	97.5

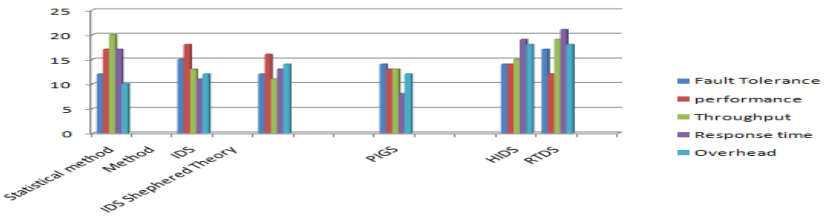
.

Table 2. Mode of Action of Detection Techniques

Name of Techniques	Objective	Deployment	Working Mode	Trainable
STATISTICAL METHOD	Attack Detection	Between Source and Destination	Centralized	No
INTRUSION DETECTION SYSTEM	Attack Detection	Intermediate	Distributed	Yes
IDS BASED DEMPSTER-SHAFER THEORY	Attack Detection	Victim Side/ Intermediate	Distributed	Yes
PACKET INFORMATION GATHERING AND PRE-PROCESSING	Attack Detection	Centralized	Centralized	No
HOST BASED INTRUSION DETECTION SYSTEMS	Attack Detection	Edge Router	Distributed	Yes
NETWORK DETECTION SYSTEM	Attack Detection	Intermediate	Centralized	No
REAL-TIME DETECTION SYSTEM	Attack Detection	Host Side	Distributed	No

4. Performance Comparison of Techniques

Though there are many techniques that have been discussed in the paper and there is the following comparison according to the comparative parameters. A technique with better performance is always preferred.



5. Conclusion

Denial of service attacks is one of the major threats on the emerging technology. Denial of service attacks aims at the using all the resources by sending fake requests in very large amount and the threat is that these requests are difficult to detect.

As IT sector is the most booming sector of the industry, so DDoS attacks have been noticed mostly in the cloud of IT industries. We discussed several intrusions or DDoS

attacks which can threat integrity, confidentiality and availability of Cloud services. Firewall only may not be sufficient to solve Cloud security issues. This paper emphasized the usage of alternative options to incorporate DDoS Detection techniques to make the cloud system secure and better. It is difficult to pre detect the DDoS attacks but not impossible. In this paper the survey of different techniques is explained and we finally identify several security challenges that need to be addressed by the research community to make Cloud a secure and trusted platform for the delivery of future Internet of Things.The main advantage of the work is that the discussed techniques have been compared on the basis of different parameters and detection can be done by comparing the different algorithms according to their parameters and the most efficient algorithm can be used for the detection purpose. If the future scope took into the consideration then it can be said that the work can be continued on their weak parameters so their performance or other parameters can be taken high in the positive manner. If the detection will be efficient then it will make the prevention easier.

References

[1] N. Singh, A. Hans, A. Sharma and K. Kumar, "Department of CSE, Guru Nanak Dev University Regional Campus", Jalandhar, India in "Unfolding various security brawls and concerns of cloud computing" international conference on Computational Intelligence on Power, Energy and Controls with their impact on Humanity (CIPECH) , **(2014)** November, pp. 28-29.

[2] K. Kumar, N. Singh, A. Hansand A. Sharma,"Department of CSE, Guru Nanak Dev University Regional Campus", Jalandhar, India in "Unfolding Towards the various cloudcomputing scheduling concerns: A review" international conference on Computational Intelligence on Power, Energy and Controls with their impact on Humanity (CIPECH) , IEEE, **(2014)** November, pp. 28-29.

[3] K. Kumar, A. Hans, N. Singh and A. Sharma, "Department of Computer Science Guru Nanak Dev University RC Jalandhar", India" Comparative Analysis of Various Cloud Based Scheduling Algorithms" International Journal of Advanced Research in Computer Science and Software Engineering, vol. 4, no. 8, **(2014)** August, ISSN: 2277 128X.

[4] N. Singh, A. Hans, A. Sharma and K. Kumar,"A Review on Security Issues in Cloud Computing", International Journal of Innovation and Applied Studies, ISSN 2028-9324, vol. 8, no. 3, **(2014)** September, pp. 1090-1093.

[5] T. Aura, P. Nikander and J. Leiwo, "Dos-resistant authentication with client puzzles", Proceedings of Security Protocols Workshop, Lecture Notes in Computer Science, vol. 213, no. 33, **(2000)**, pp. 170-181.

[6] A. Chonka,W. Zhou and J. Singh,"Chaos theory based detection against network mimicking DDoS attacks", IEEE Communications Letters, vol. 13, no. 9, **(2010)**, pp. 717–9.

[7] Y. Feng, R. Guo, D.Wang, and B. Zhang, "A comparative study of distributed denial of service attacks, intrusion tolerance and mitigation techniques, intrusion tolerance and mitigation techniques", In Proc. of the 5th International Conference on Natural Computation (ICNC'09), Tianjian, China,. IEEE, **(2009)** August, pp. 628–632.

[8] S. Suriadi, D. Stebila, A. Clark and H. Liu, "Defending web services against denial of service attacks using client puzzle", In Proc. of the 9th International Conference on Web Services (ICWS'11), **(2011)** July, pp. 25–32, Washington DC, USA.

[9] http://www.neustar.biz/resources/whitepapers/2014-neustar-ddos-report

[10] M. H. Bhuyan, H. J. Kashyap, D. K. Bhattacharyyaand J. K. Kalita, "Department of Computer Science & Engineering", Tezpur University, Napaam, Tezpur-784028, Assam, India[2]Department of Computer Science, University of Colorado at Colorado Springs, CO 80933-7150, USAEmail: {mhb,dkb}@tezu.ernet.in, jkalita@uccs.edu

[11] Y. Chen, K. Hwang and W. S.Ku,"Distributed change-point detection of DDoS attacks over multiple network domains", Proceedings of the IEEE International Symposium on Collaborative Technologies and Systems, Las Vegas, NV, IEEE CS, vol. 14-17, **(2006)** May, pp. 543–550.

[12] A. M. Lonea, D. E. Popescu, "TianfieldDetecting DDoS Attacks in Cloud Computing Environment", INT J COMPUT COMMUN, ISSN 1841-9836 8, no. 1,**(2013)** February, pp. 70-78.

[13] C. C. Lo, C. C. Huang and J. Ku, "A Cooperative Intrusion Detection System Framework for Cloud Computing Networks", In 39th International Conference on Parallel ProcessingWorkshops, **(2010)**, pp. 280-284.

[14] J. Choi, C. Choi, B.Ko, D. Choi, and P. Kim,"Chosun University", Gwangju, Republic of Korea xdman@paran.com, fenduaranceaura, byeongkyu.ko, dongjin.choi84g@gmail.com, pkkim@chosun.ac.kr

[15] C.Modi, D. Patel, B. Borisaniya, H. Patel, A. Patel, M. Rajarajan and N. S. Gujarat,India [2]S.P. CollegeofEngineering,Gujarat,India; [3]City UniversityLondon,UK "A survey of intrusion detection

techniques in Cloud" Elsevier Journal of Network and Computer Applications, vol. 36, **(2013)**, pp. 42–57.
[16] Z. Muda, W. Yassin, M.N. Sulaiman, and N.I. Udzir, "Intrusion detection based on K-Means clustering and Naïve Bayes classification", 7th International Conference on Information Technology in Asia, Emerging Convergences and Singularity of Forms (CITA), **(2011)**.
[17] T. Komviriyavut, P. Sangkatsanee, N. Wattanapongsakorn, and C. Charnsripinyo, "Network intrusion detection and classification with decision tree and rule based approaches", 9th International Symposium on Communications and Information Technology (ISCIT), **(2009)**, pp. 1046-1050.

Author

Navdeep Singh, Born on Sept 8 1990 in Dasuya city District Hoshiarpur Punjab India. Completed his B Tech (CSE) from BCET Gurdaspur in year 2012 and Pursuing M.Tech in computer Science and Engineering GNDU Regional Campus Jalandhar, Punjab. Area of interest in technology is Cloud Computing, Security brawls of Cloud Computing, Encryption and Decryption. Many research papers have been published of the author in the different conferences like IEEE and different Journals. Looking forward to go for Doctorate in the same field to continue his research.

