A Review of Techniques to Detect and Prevent Distributed Denial of Service (DDoS) Attack in Cloud Computing Environment

Iqra Sattar
Department of Computer Science
University of Lahore (Sargodha)

Muhammad Shahid
Department of Electrical Engineering
PIEAS, Islamabad

Younis Abbas
Department of Computer Science
University of Lahore (Sargodha)

ABSTRACT
Cloud computing has become one of the most demanding services over the internet. It has gained remarkable fame for past few years.But it is under the severe threats of internet security. One of the severe threats is Distributed Denial of Service (DDoS). DDoS occurs when a huge amount of packets are sent to a server from various computers. Botnet is one of the major causes that launch DDoS attack. Botnet is actually a network of bots or zombie computers that are under the control of attacker. Several techniques are available in the literature that provides solution to avoid DDoS attack.A survey on DDoS detection and prevention techniques and their comparative analysishave been done in this paper.

Keywords
DDoS, Botnet, CBF, Cloud Computing, TTL, DST.

1. INTRODUCTION
Cloud computing is a model to deliver on demand computing resources with the minimal effort and management [1, 2]. It is the sharing the computer resources over the internet. These shared resources can be in the form of software, development interface, virtual hardware or storage. The essential components of a cloud computing are Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). These resources are dynamic and can be configured according to the needs.

As cloud computing provide large amount of resources online, so it is facing with several security problems like secrecy, authenticity, confidentiality and DDoS attack. The most major threat to Cloud security is Distributed Denial of Service Attack (DDoS) [22]. DoS attack greatly affectthe services of simple network and there are different techniques for its detection and prevention, this attack also affect the new emerging cloud computing technology, so to improve resource availability of resources in cloud computing environment, it is essential to provide a mechanism to prevent DDoS attacks [24].

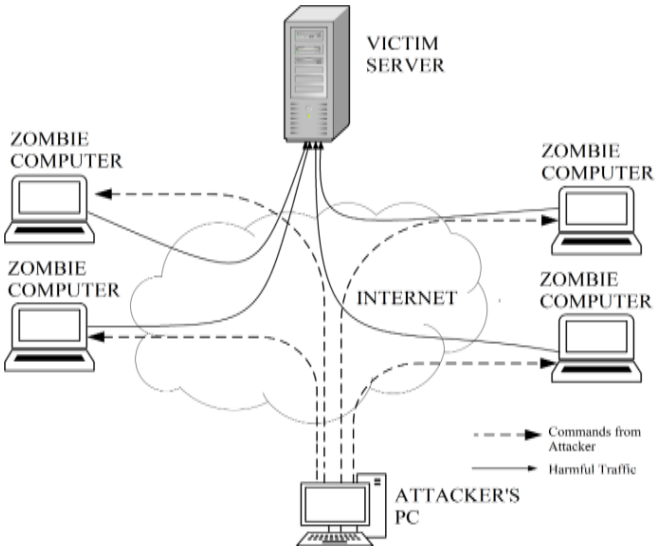

Fig1: DDoS Attack

Distributed denial of service (DDoS) occurs to a server when attacker sends a huge amount of fake packets from a number of zombie computers which are already under the control of attacker. DDoS have become a serious problem and the attackers are also using sophisticated ways to target the victims. A number of defense mechanisms are proposed to avoid DDoS attacks [12, 13].

The DDoS attacks can be launched from multiple environments, likefromsome specific service,virtual machine, some node, some cluster or in the whole cloud environment.In this article we present different DDoS attack detection and prevention techniques at different levels [26].

The rest of the article is organized in the following way: the background is discussed in section II, all the literature survey on DDoS attacks detection and prevention techniques is discussed in Section III, the comparative analysis between the techniques are discussed in section IV, Section V mentions about Conclusion of this paper and Section V describes further enhancement and Future Scope.

2. BACKGROUND

Internet security is the major concern in Cloud computing. These are several threats to Cloud computing such as worms, spams, phishing attacks etc. Recently, a new severe threat has come to light know as Botnet. Botnets are the main cause of malicious activity in the Cloud computing. Attacker sends malicious content to the computer over the internet. Once those computers become victim of Botnet, they act like a bot for the attacker [23]. These bots form network that being controlled by the attacker. Several malicious activities can be formed using Botnet like leakage of sensitive information etc. but one of the severe attacks is DDoS [21].

In DDoS attack, when a huge number of queries come to the server, the server increases its computational power and starts to entertain every request. The server system has the limited capacity to entertain the number of user request at a time. So, when a huge a number of fake request or queries come to the server, the server gets busy and the actual user request cannot be entertained in that period. Hence the denial of service occurred [25].Usually, the cloud network is a distributed system, therefore, distributed denial of service happens more often [20].

In order to prevent from DDoS attack in cloud computing environment, different techniques for DDoS detection and prevention has been discussed in this paper, the terminologies used in them are discussed below.

i. Hop Count Computation: The hop-count is not available in the IP header. It is computed using Time-to-Live (TTL) information. TTL is an 8-bit field in the IP header for the purpose of maximizing the life of data packet over the internet. The router updates this field and forwards this packet to the next hop [6, 14].

ii. IP2HC Table: The IP2HC table is very useful to confirm the hop count. IP2HC table contains the information about the source IP and hop count of that IP for a received packet [15].

iii. Confidence Based Filteringmethod: CBF is based on the correlation patterns. The correlation patterns are evaluated from a sampled data depending upon some characteristics.A database is established on the server to store the outcomes. This storing feature helps to detect a certain pattern but it also reduces the processing speed.

iv. Confidence is measure of repetition of certain pattern in a packet flow. It can be calculated as:[7]

Confidence for single attribute[16]:

$$Conf(A_i = a_{i,j})_{single\ attribute} = \frac{N(A_i = a_{i,j})}{N_n}$$

Confidence for pair attribute[16]:

$$Conf(A_{i1} = a_{i1,j1}, A_{i2} = a_{i2,j2})_{pair\ of\ attributes} = \frac{N(A_{i1} = a_{i1,j1}, A_{i2} = a_{i2,j2})}{N_n}$$

v. Dempster Shafter Theory (DST):Dempster combination rule is modified to fuse the results of different independent sources using AND operation.

vi. Intrusion Detection System:An IDS is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a management station.

3. LITERATURE REVIEW

In this section differentDDOS attack detection and prevention techniques for cloud computing environment proposed by different authors has been collected and discussed.

3.1 Packet Monitoring TTL Approach

In the proposed algorithm, hop count filtering (HCF) technique is used to detect the DoS attack in a cloud network. It is deployed at cloud environment. In this algorithm, the data packets are monitored continuously over the cloud network and three parameters are extracted from that packets, a) SYN flag, b) TTL and c) Source IP [17]. There are four possible scenarios for each packet evaluation:

i. If a data packet is received and there is information of IP2HC table. Extract the parameters such as SYN flag, source IP and TTL. If the source IP is already available in the table and SYN flag isHIGH then calculate hop-count using TTL information. If the calculated hop-count matches with stored value of hop-count in IP2HC table then do nothing. Otherwise, update the stored hop-count field in IP2HC table with this new hop-count for that source IP. [4]

ii. If the SYN flag is HIGH but the source IP does not exist in IP2HC table then calculate the hop-count, add a new entry for this new IP and store the calculated hop-count for the corresponding IP in IP2HC table.

iii. If the SYN flag is LOW and source IP exist in the IP2HC table, then calculate the hop-count. If the calculated hop-count matches with the existing hop-count of IP2HC table for the corresponding IP then this packet is real otherwise this packet is spoofed.

iv. If the SYN flag is LOW and the source IP information is also not present in IP2HC table then it is sure that this received packet is spoofed because every genuine packet always contains valid IP information of the source in IP2HC table.

This algorithm only needs information of SYN, source IP and TTL. Using TTL value, hop-count is calculated which is then compare with the stored of value of hop-count of IP2HC table. Using only these three parameters, the authenticity of a received data packet is analyzed. Hence on detection of spoofed data packets, the server simply ignores that packet and be ready to serve a genuine user [5]. Its drawback is that the algorithm requires continuous monitoring of packets travelling over the network in the Cloud.

3.2 Entropy based Anomaly Detection

Entropy or Shannon-Wiener index theory is an important theory to analyze the random data. It is used to determine the uncertainty or randomness associated with data. Entropy is measure of randomness. More randomness in the data means more entropy. If the data belongs to one class, the entropy will be lesser and if the data belongs to many classes, the entropy will be larger. So, the headers of sampled data are analyzed for IP and Port and their entropy is computed [6] [18].

The entropy will be minimum if the data is coming from one IP or Port. IP or Port both can be used to compute the entropy. If only IPs are used for computation of entropy then the maximum value of entropy will for IPV4. If the Ports are also used then the maximum value of entropy will be very large. The change in entropy will show that the traffic is coming from different sources. A threshold can be defined to detect the DDoS attack. If the entropy increases beyond that threshold, the system should generate an alarm of DDoS attack.

For multilevel DDoS detection, the process can be divided into two steps:

i. First time, the user is allowed to pass through the router and Detection algorithm verifies the user that it is genuine.

ii. Second time, the try to pass through the router, the entropy is computed depending upon the data packet size and user's authenticity. If the computed does not meet the standard range, it is considered as intruder and a message it sent to the Cloud Service Provider.

iii. The entropy of each data packet is calculated and compared with the threshold value. On detection of any anomaly, a message is sent to the Cloud Service Provider (CSP) for necessary action.

3.3 CBF Packet Filtering Method

In the proposed method, a modified CBF (Confidence Based Filtering) method is introduced to reduce the storage needs and to increase the processing speed on the server side. It is deployed at cloud data base. This technique is also based on correlation patterns. Since the confidence value is stored in the optional fields of IPV4 header, therefore, a 32bit word is added in IPV4 header.

The amount of trust that can be assigned to a correlation pattern between an attribute pair, is well described in [8].

For enhanced CB, the legitimate packet is the one which has the confidence value (CV) above the threshold value. If the packet does not attain a CV above the threshold, it is discarded. In this algorithm the nominal confidence values that is stored in the profile, is used as threshold value and the confidence of each incoming packet is calculated and compared with the threshold confidence value. If the incoming packet has greater confidence value than the threshold value then it is accepted. Otherwise it is discarded.

3.4 Intrusion Detection System using Dempster Shafter Theory

The proposed technique includes Cloud Fusion Unit (CFU) which collects the alerts from different IDS (Intrusion Detection System) sensor VMs (Virtual Machines). The alerts will be stored into the Mysql database of Cloud Fusion Unit. This Cloud Fusion Unit will analyze the results using the Dempster-Shafer theory (DST) of evidence in 3-valued logic and it will apply the Fault-Tree Analysis for each IDS sensor VMs. The results of the sensors are fused using Dempster's combination rule. This technique is deployed at node [9] [19].

For detection and analysis of Distributed Denial of Service (DDoS) attacks in cloud computing, a virtual cloud is setup with frontend and three nodes. The detection is carried out using pre-configured Intrusion Detection Systems (IDSs) installed in virtual machines (VMs). The assessment phase is carried out in the frontend using Cloud Fusion Unit (CFU). Snorts are installed and configured into each VM to realize IDS[10] [11].

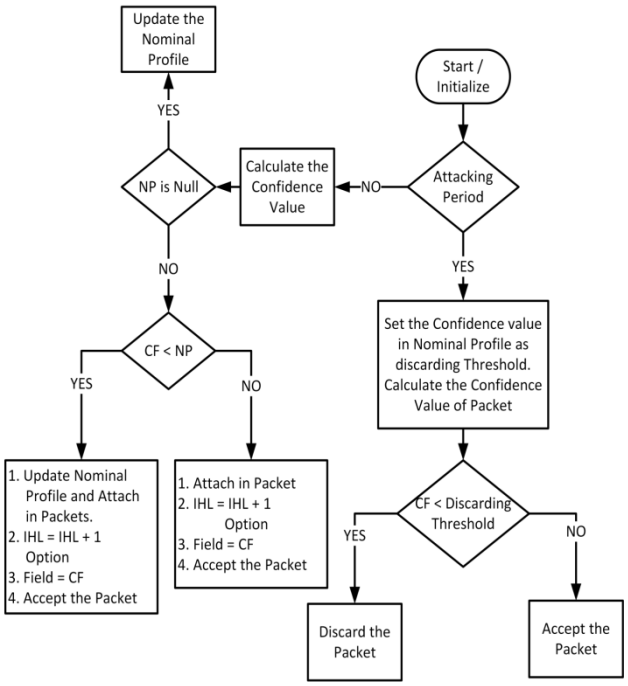

Fig2: DDoS Attack

The detection is carried out using pre-configured Intrusion Detection Systems (IDSs) installed in virtual machines (VMs).The alerts are then analyzed using Dempster-Shafer theory of evidence in 3-valued logic and converted into Basic Probabilities Assignments (bpas).

After obtaining the probabilities for each attack packet, the probability for each VM-based IDS is calculated using the fault-tree. This DST with fault tree analysis helps to calculate the authenticity of the attack for each VM. Finally for assessment, Dempster's combination rule is used to maximize the true DDoS attack alerts.

4. COMPARATIVE ANALYSIS OF TECHNIQUES

In comparative analysis we have compared techniques that are discussed earlier. We found that each technique some pro and cons. Some techniques are deployed on node, some on VM and some on cloud database.

Table 1.Comparative Analysis of DDoS Attack Detection & Prevention Techniques

Technique	Deployed	Pros	Cons	Remarks
Packet monitoring TTL	Cloud Node	Detect DDoS attack in cloud	Monitoring of packets continuously slow down the performance	Whole traffic should not be allowed directly to node.
Entropy Based Anomaly Detection	Cloud Gateway	Detect DDoS attack at cloud gateway	Entropy calculation of each packet is overhead	…….

CBF Packet Filtering Method	Cloud Database	Detect DDoS attack on Cloud Database	Reduce processing speed	…….
Intrusion Detection System Using Dempster Shafter Theory	Virtual Machine	Detect DDoS attack on Cloud VM	Generate large no of alert which slow down the performance	Exception generated should be updated on Node or Cluster.

5. CONCLUSION

In this paper a survey of different techniques for detecting and preventing DDOS attack in cloud computing system, and the comparative analysis among them has been discussed. Cloud Computing is gaining popularity, but with the widespread usage of cloud, the issue of cloud security is also surfacing. One of the major threats to Cloud security is Distributed Denial of Service Attack (DDoS) or simply Denial of service attack (DoS). To improve availability of resources, it is essential to provide a mechanism to prevent DDoS attacks.

6. FUTURE WORK

In "Intrusion Detection System Using Dempster Shafter Theory" exception are generated at VM which slow down performance. There is possibility if we develop such mechanism in which exception generated by VM are updated at Node/Cluster so that next time such exception should be entertained at cloud node or cluster level.

7. ACKNOWLEDGMENTS

Thanks to Allah Almighty for His mercy and blessings and all those who have contributed in this paper.

8. REFERENCES

[1] M. Ahmed, X. Yang, and S. Ali, "Above the Trust and Security in Cloud Computing: A Notion Towards Innovation," in Embedded and Ubiquitous Computing (EUC), IEEE/IFIP 8th International Conference, 2010, pp. 723-730.

[2] I. Gul, A. urRehman, and M. H. Islam, "Cloud computing security auditing," in Next Generation Information Technology (ICNIT), 2011 The 2nd International Conference on, 2011, pp. 143-148.

[3] VikasChouhan&Sateesh Kumar Peddoju "Packet Monitoring Approach to Prevent DDoS Attack in Cloud Computing" International Journal of Computer Science and Electrical Engineering (IJCSEE) ISSN No. 2315-4209, Vol-1 Iss-1, 2012.

[4] P. A. R. Kumar and S. Selvakumar, "Distributed Denial-of-Service (DDoS) Threat in Collaborative Environment - A Survey on DDoS Attack Tools and Traceback Mechanisms," in Advance Computing Conference, 2009. IACC 2009. IEEE International, 2009, pp. 1275-1280.

[5] W. Haining, et al., "Defense Against Spoofed IP Traffic Using Hop-Count Filtering," Networking, IEEE/ACM Transactions on, vol. 15, pp. 40-53, 2007.

[6] A.S.SyedNavaz, V.Sangeetha, C.Prabhadevi. "Entropy based Anomaly Detection System to Prevent DDoS Attacks in Cloud" International Journal of Computer Applications (0975 – 8887) Volume 62– No.15, January 2013.

[7] PriyankaNegi, Anupama Mishra and B. B. Gupta."Enhanced CBF Packet Filtering Method to Detect DDoS Attack in Cloud Computing Environment".

[8] Qi Chen, Wenmin Lin, Wanchun Dou, Shui Yu, "CBF: A Packet Filtering Method for DDoS Attack Defense in Cloud Environment", in Ninth IEEE International Conference on Dependable, Autonomic and Secure Computing, 978-0-7695-4612-4/11, 2011.

[9] A.M. Lonea, D.E. Popescu, H. Tianfield. "Detecting DDoS Attacks in Cloud Computing Environment", INT J COMPUT COMMUN, ISSN 1841-9836 8(1):70-78, February, 2013.

[10] Roschke, S., Cheng, F. and Meinel, C., "Intrusion Detection in the Cloud". In Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing, pp. 729-734, 2009.

[11] Dissanayake, A., "Intrusion Detection Using the Dempster-Shafer Theory". 60-510 Literature Review and Survey, School of Computer Science, University of Windsor, 2008.

[12] J. Mirkovic and P. Reiher; A Taxonomy of DDoS Attack and DDoS Defense Mechanisms; ACM Sigcomm Computer Communications Review; Vol. 34, No. 2, Apr. 2004.

[13] Chen R. , Park J., and Marchany R., " A Divide and Conquer Strategy for Thwarting Distributed Denial of Service Attacks," Computer Journal of IEEE Transactions on Parallel and Distributed Systems, vol.18, no. 5, pp. 577-588,07

[14] I. B. Mopari, et al., "Detection and defense against DDoS attack with IP spoofing," in Computing, Communication and Networking, 2008. ICCCn 2008. International Conference on, 2008, pp. 1-5.

[15] N. Venkatesu, et al., "An Effective Defense Against Distributed Denial of Service in GRID," in Emerging Trends in Engineering and Technology, 2008. ICETET '08. First International Conference on, 2008, pp. 373-378.

[16] Qi Chen, Wenmin Lin, Wanchun Dou, Shui Yu, "CBF: A Packet Filtering Method for DDoS Attack Defense in Cloud Environment", in Ninth IEEE International Conference on Dependable, Autonomic and Secure Computing, 978-0-7695-4612-4/11, 2011.

[17] H. Wang, C. Jin, and K.G. Shin, "Defense against Spoofed IP Traffic Using Hop-Count Filtering, inIEEE/ACM Trans. Networking, vol.15, no.1, 2007 pp.40-53.

[18] Chonka, J. Singh, and W. Zhou, "Chaos Theory Based Detection against Network Mimicking DDoS Attacks," in IEEE Comm. Letters, vol. 13, no. 9, 2009, pp.717 -719.

[19] Y. Kim, W. C. Lau, M. C. Chuah, and H. J. Chao, "PacketScore: A Statistics-Based Packet Filtering Scheme against Distributed Denial of-Service Attacks," in IEEE Trans. Dependable and Secure Computing ,vol. 3, no. 2, 2006, pp.141-155.

[20] B. B. Gupta, R. C. Joshi, M. Misra, "Defending against Distributed Denial of Service Attacks: Issues

and Challenges," Information Security Journal: A Global Perspective, vol. 18, issue 5, Taylor & Francis, UK, pp. 224-247, 2009. DOI: 10.1080/19393550903317070

[21] Y. Xiang, K. Li, and W. Zhou, "Low-Rate DDoS Attacks Detection and Traceback by Using New Information Metrics," in IEEE Trans. Information Forensicsand Security, vol. 6, no. 2, 2011, pp.426-437.

[22] B. B. Gupta, M. Misra, R. C. Joshi, "FVBA: A Combined Statistical Approach for Low Rate Degrading and High Bandwidth Disruptive DDoS Attacks Detection in ISP Domain," in the proceedings of 16th IEEE International Conference on Networks (ICON-2008), DOI: 10.1109/ICON.2008.4772654, Dec. 12-14, 2008, New Delhi, India.

[23] B. B. Gupta, R. C. Joshi, ManojMisra, "ANN Based Scheme to Predict Number of Zombies involved in a DDoS Attack," International Journal of Network Security (IJNS), vol. 14, no. 1, ISSN 1816-3548, pp. 36-45, 2012.

[24] P.E. Ayres, H. Sun, H. J. Chao, and W. C. Lau, "ALPi: A DDoS Defense System for High-Speed Networks," in IEEE J. Selected Areas Comm., vol. 24, no. 10, 2006, pp.1864 -1876.

[25] EsraaAlomari, SelvakumarManickam, B. B. Gupta, Shankar Karuppayah, RafeefAlfaris, "Botnet-based Distributed Denial of Service (DDoS) Attacks on Web Servers: Classification and Art," in International Journal of Computer Applications, (IJCA), Vol. 49, no. 7, pp. 24-32, 2012.

[26] A. Srivastava, B.B. Gupta, A. Tyagi, A. Sharma, A. Mishra, et. al., "A Recent Survey on DDoS Attacks and Defense Mechanisms," Book on Advances in Parallel, Distributed Computing, Communications in Computer and Information Science (CCIS), LNCS, Springer-Verlag Berlin Heidelberg, CCIS 203, pp. 570-580, 2011.