Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 5.258

IJCSMC, Vol. 5, Issue. 7, July 2016, pg.136 – 141

A Review on DOS and DDOS Attacks in Cloud Environment & Security Solutions

Tanshu Gairola[1], Kulvinder Singh[2]

Computer Science, Uttarakhand Technical University, India

[1] tanugairola@gmail.com; [2] kulvinder.taak@gmail.com

Abstract— Cloud computing, just a buzz word few years ago, has lead in a new way of computing that leverages networks and operating software to provide virtually unlimited computing capability whenever it is needed – and that includes Internet of Things applications, Cloud and the Internet of things are inextricably linked. Trend of using cloud computing in the field of Information Technology to deal with providing scalable and flexible facilities to the customers as per demand is emerging these days. Cloud computing compromises services in three levels known as infrastructure, platform and software to deal with the requests of variety of customers. The simple cloud characteristics enclose with multi tenancy, location and device independence, elasticity, resource pooling and measured service. The IT enterprises mainly the Small and Medium Scale companies are going towards the cloud which empowers them to complete high end computational tasks in a budget. As the use of theses service increases the more there is security concern because the more number of IT capabilities provided as a service in cloud, the more the risk in security is concern. From the various attacks that can deal with the cloud environment, DoS or DDoS attacks can reason a major breach in security. For dealing with DDOS attacks there are various techniques and methods which are based on associated condition of the situation that can be further categorized as Prevention, detection and reaction that is after effects. More precisely this leads from avoiding occurrence of DDOS, appropriate solutions to detect when it occurred and accurate technique to handle this denial of service attacks without getting system services unattainable by user. This paper discuss about the numerous DDOS attacks and the defense mechanisms that can be taken place to secure the cloud.

Keywords— Cloud Computing, WSN, Counter methods, DDOS, IPV6, IOT, DDOS attack, Flooding.

I. INTRODUCTION

Technology has gone through a big boost in the recent year. The acceptance of services by Cloud service provider has greater than before as compare to the past few years. There is couple of threats that should be known by Cloud service providers and their customers should be alert of. Enterprises that have been running their own data canters and web properties, these threats will be familiar and come as no surprise; attacks on the global Domain Name System (DNS) infrastructure and Distributed Denial of Service (DDoS) attacks are something that proprietors of Internet-connected IT infrastructures and Cloud services, big and small, need to be aware of and plan for in order to manage the risk of interruption to their operations. These attacks have the potential to disturb Internet services such as online facilities, browsing websites, portals, and Cloud services, and also infect the devices connected over internet with malware that deal with those internet services. Organizations that operate or use Internet connected services such as websites, portals and Cloud services need to be aware of threats that can disrupt service.

A. Distributed Denial of Service(DDOS) attacks

A denial of service is characterized by an explicit attempt by an attacker to prevent authenticate users from using computing resources. DDOS attack deal with those zombie computer that are actually the infected computer. Sometimes a cracker usages a connection network of zombie computers to sabotage a precise Web site or server. The idea is pretty simple a cracker tells all the computers on his botnet to contact a particular server or Web site continually. The rapid growth in traffic can reason the site to load very slowly for valid users. Sometimes the traffic is adequate to shut the site down totally. We call this type of an attack a Distributed Denial of Service (DDoS) attack. Some mainly tricky botnets use uncorrupted computers as part of the attack. An attacker may attempt to: "flood" a network and thus decrease a genuine user's bandwidth, disrupt service to a particular system and a user prevent right to use to a service. In the networks Distributed Denial of Service (DDoS) attacks needs to be prevented or handled if it occurs, as early as possible and before reaching the victim. Dealing with DDoS attacks is difficult due to their properties such as dynamic attack rates, various kinds of targets, big scale of botnet, etc. Distributed Denial of Service (DDoS) attack is hard to deal with because it is difficult to distinguish legitimate traffic from malicious traffic, especially when the traffic is coming at a different rate from distributed sources. DDoS attack becomes more difficult to handle if it occurs in wireless network because of the properties of ad hoc network such as dynamic topologies, low battery life, multicast routing, frequency of updates or network overhead, scalability, mobile agent based routing, and power aware routing, etc. Therefore, it is better to prevent the distributed denial of service attack rather than allowing it to occur and then taking the necessary steps to handle it.

B. DoS & DDOS Attacks in Cloud Environment

With reference to cloud computing there are well known two main availability related attacks:

- Denial of service (DoS)
- Flooding.

These both attack effect the available Distributed Denial of Service attack, broadly known as DDoS attack, is the primary threat to cloud computing. The DDoS threats effort to create the online data unobtainable by readdressing irresistible traffic, from several resources. The tendency of the threat is varying across accommodations. DDOS threats perceived growth of 132.43% in Q2 2015 as compared to the previous quarter last year, with China being the topmost basis of the outbreak, accounting for 37.01%, followed by the US and the UK. China is the major committer as well as the goal of these threats or attacks. Brazil appeared as the different hub of hackers accounting to 11% of all attacks. The survey report done by Akamai on the other hand claims that the biggest DDoS attack occurred at 240 gigabits per second, which continued for more than 13 hours. Though, the top bandwidth attack happened only for about two hours. The Q2 report [21] by Akamai claims the Gaming Sector to be the worst hit, with more than 35% of attacks faced by it. The sector is followed by Software and Technology at 28%, and Internet and telecom at 13%. Besides, from the financial services, Banks and trading platforms accounting for 8% of attacks and see few larger attacks of 100+Gbps of the quarter. Most of the individual customer attacks in the financial services industry are found to be Shellshock attacks. However, an article at TCS website claims banking industry is the main victim of attacks, struggling to counter them. Devising a strategy though may not be an easy job, as no two DDoS attacks are alike.

C. Factors affecting DDOS attack

One of the main reasons that mark the DDOS attacks well-known and easy in the cloud is the availability of all tools that deal with DDOS attack and the powerfulness of these tools to produce massive capacities of attacking traffic.

The following are the opportunities for the attackers to work attack tools easily to launch attack:

- Internet security is extremely interdependent the launch of DDoS attack based upon the global internet security.
- Limited Internet resources, Every Internet host have restricted resources that can be obsessive by an enough digit of customers.
- Control is distributed; sometimes it is closely impossible to examine the cross network behavior and to set out certain worldwide security tool due to confidentiality concerns of the Internet.
- Multipath routing, this causes authentication procedure problematic and that may leads to unauthorized actions. Intermediate router straight on IP packet from source to destination without information about the IP packet whether it is honest or not.

II. PROBLEMATIC MIXTURE OF IOT,IPV6 AND DDOS

IOT is next phase of internet i.e. the internet of things that deal with sensor and connected device , that are ubiquitous popping up and the data they are producing has to be processed somewhere. While the simple stuff and the immediate stuff happen locally, more complex –predictive analytics, visualizing data – happens in the cloud. IPV6 is internet protocol version 6 that deals with the concept of providing address as the number of

users connected to internet has crossed the IPv4 Limit. IOT needs the enormously expanded protocol address space that only IPv6 can provide. But this IPV6 for IOT raise the series of security concern that includes massive potential expansion for distributed denial-of-service (DDoS) attacks that also comes in existence. The Internet is flooded with fresh things, and the arrival of IPv6 and the Internet of Things (IoT), could potentially lead to a whole lot of concern. There is a possibility that the billions of IoT devices, flooding the Internet and this new addressing scheme, which is required to accommodate the burst of wireless technology, will form a landscape that lets malicious hackers or attackers to launch potentially potent distributed denial of service (DDoS) attacks. While IPv6 will certainly help in fitting in with the growth of new connected phenomena, such as IoT, adoption at the instant is slow. And due to this version of internet protocol (IPv6) that take up such a relatively small space, Internet security implementations that take it into full consideration are also gets floppy. This leads to occurrence of DDOS attacks in networks. Basically DDoS attacks occur when hackers on internet use infected hosts to regulate connected devices remotely and by using infected devices (bots) send malicious traffic to their target their victim, for targeting a system's organizations victim are flooded with traffic, thus restricting or disabling service for legitimate traffic, or crashing the victim network. DDoS attacks direct traffic to a particular Internet address, and today the vast majority of those addresses are handled by Internet Protocol version 4, or IPv4. IPv6, which vastly increases the number of possible addresses to deal with the fact that IPv4 is running out of them, is gradually becoming a reality as those with servers and network gear invest in the new network.

IPv6 is not the main course for attacks, since it is still a relative backwater, but two difficulties make IPv6 particularly vulnerable. First, with the relatively not fully formed network infrastructure, many network operators do not have the capability to pore over network traffic well enough to make a distinction DDoS attacks from benign traffic. Second, gateways that link IPv4 and IPv6 must store lots of "state" information about the network traffic they handle, and that essentially makes them more brittle. Gateways between IPv4 and IPv6 that are frail and precarious; and the unprecedented spreading of relatively unsecure IoT devices, loaded with those new IPv6 vulnerabilities, all creating everywhere potential fuel for botnets. Investments in counteract a danger are costly but so are DDoS attacks.

A. The Impact : Direct & Indirect

DDOS attack is an attempt to consume finite resources without any need, benefits from weakness in design and affect the availability of service by exploiting the capacity. The main challenge is to maintain availability in case of attack. Service availability is directly proportional to business. There are different kind of impact of DDOS attack the first one Direct Denial of Service, When in Cloud Computing environment if a system notices the high workload during computation on the particular service then to deal with this additional workload it will start to facilitate more computational power like virtual machines, service instances. Cloud defence systems try to work against the attacker. Second is Indirect Denial of Service fall under the situation when the Computational power in control of the attacker, drawback of the direct flooding attack is that the other cloud services facility that take place in same platform may have to suffer with workload by this flooded traffic. Hereby, if a service takes place to run on the same server with another, flooded service instance, this can affect its own accessibility as well**.** Furthermore impact deal with Accounting cloud computing service that is charging as per the customers' requirements, as per the actual usage of resources; Symptoms of DDOS include unusually slow Network Performance, unavailability of legitimate user's services, Inability to access any Website, Unavailability of particular Website, and Dramatic Increase in the No. of Spam E-mail. Other major outcome of a flooding attack is raising bills for Cloud usage extremely as on cloud services, having no "upper limits" to computational power usage is the real issue.

III. TECHNIQUES TO COUNTER DDOS ATTACKS

Here is an overview of important technologies to know about for context around big data infrastructure.

A. Key Points for Selecting Defence Solution

Before selecting any DDoS detection prevention techniques there are some points that need to be considered to achieve the effective solution.

These are:

- Functional: The solution should be capable to decrease impact of the attack irrespective of how powerful the attack is.it should be dynamic enough so that it can maintain the availability of services when faces an attack.
- Simple and Apparent: The solution must be easy to implement i.e. it should not require modifying the existing network and its infrastructure.
- Lightweight: By applying heavy mechanism the solution overhead the system that effect the system performance so need the lightest solution.

- Accuracy: The accuracy of technique also important so that it does not give lots of false positive.as in some techniques there is a need to be dropped or discarded the traffic but the solution must not drop genuine traffic.

B. Review Techniques to counter DDOS Attack

There are different methods and techniques to counter DDOS attacks. Some traditional methods to defence DDOS include trace back or packet filtering approaches and others deal with traffic analysis, neural network solution, application layers DDOS defence mechanism etc.

1) Co-operative Intrusion Detection System: There are various DDOS detection technique that deal with ID system .A Snort based DIDS is set up in each cloud computing region which will cooperate with each other to mitigate the influence of DDoS attack in the network. The IDS compares the type of expected packet with that in its block table and if a match is found, the packet is released immediately. If no match is found, but detected as anomalous then there is an alert notice is sent to all other IDSs. Each ID interchange alerts with other IDS and uses the majority vote method to choose true and false alerts. If alert is true, then the block table is updated with new block rule to identify such kind of attacks in the future. The IDS contains of four components to perform the detection namely intrusion detection, alert clustering and threshold computation and comparison, intrusion response and blocking and cooperative operation [10]. The IDS helps in early detection and prevention of DDoS attack in a cloud environment with more computational time.

2) Confidence Based Filtering (CBF) Approach: This approach works on two periods namely a non-attack period and an attack period. Confidence based filtering method is used to prevent DDOS at transport and network layer of cloud environment. A correlation patterns are used to calculate CBF value of incoming packet. A packet is divided into attack period and non-attack period .If it is in non-attack period then confidence value which is calculated updates the nominal profile of legitimate users .If it is in attack period then it looks up for nominal profile value and confidence value is compared with CBF score which is decided whether to discard or pass the packets. During a non-attack period, it identifies unique correlation patterns among legitimate packets by extracting attribute pairs in their IP and TCP headers. Then it calculates a confidence value to determine the trustworthiness of a particular correlation pattern between an attribute pair. Higher the frequency of an attribute pair during normal packet flow, the higher the confidence value it can get. This dataset can be called as a nominal profile. During an attack period, CBF score for each packet is calculated which is the weighted average of confidence values of attribute pairs in it. Then the CBF score is compared with discarding threshold to decide whether the packet is legitimate or not. If CBF score is higher than the threshold, the packet is legitimate and allowed to pass or else the packet is discarded [12]. The merits of CBF method includes less storage space and high computational speed and efficiency which makes it suitable for large network traffic.

3) Filtering Tree Approach: This approach is very useful to curb HDoS and XDoS attacks in application layer. The client request is converted to XML format and then the SOAP message is doubly signed and embedded with client IP address, client puzzle and puzzles solution. Then the SOAP message is forwarded to IP trace back which compares the incoming IP address with that stored in its table. If a match is found, the packet is discarded or else it is forwarded to Cloud Defender. The Cloud defender filter the attack packets with the aid of five filters namely sensor filter, hop count filter, IP Frequency Divergence Filter, Puzzle Resolver Filter and Double Signature Filter [14]. The method fails to identify DDoS attacks in transport and network layers of the cloud.

4) Cloud Trace Back Model (CTB) and Cloud Protector: The Cloud Trace Back (CTB) is used to identify the source of the DDoS attack and Cloud Protector helps to distinguish and filter these attack patterns in the future. CTB is based on Distributed Packet Marking Algorithm (DPM) and Cloud Protector uses back propagation neural network to separate illegal message patterns. CTB is placed before the web server to avoid direct DDoS attacks [11]. The efficiency of the model depends on the efficiency of the neural network and hence training data set plays a vital role in deciding the performance of CTB.

5) CLASSIE Packet Marking Approach: CLASSIE is an IDS based on decision tree classification system which helps to prevent HX-DoS attacks, a combination of HDoS and XDoS attacks. CLASSIE is placed in one-hop distant from the host and uses it rules set to identify malicious packets. The packets will be marked after evaluation by CLASSIE and marking will be carried out by edge and core routers. The Reconstruction and Drop (RAD) which is placed one-hop back from victim makes the decision whether to allow or drop the packet. Thus the malicious packets will be marked at the attacker's end and dropped at the victim's end [13].

This method significantly reduces the overhead in packet marking and false DoS attack rates.

6) Information Theory Based Metrics Method: This method works in two phases, behaviour monitoring and behaviour detection. In the first phase, normal web user behaviour is identified during non-attack period and an entropy value for requests per session is calculated and a trust score is assigned to each user. During behaviour detection phase, the entropy value for each request is calculated and compared with a threshold value. If it exceeds the threshold value, then the request packets are considered malicious and dropped immediately. If calculated entropy is less than threshold, and then based on the trust score of the user and difference in entropy value, the rate delimiter restricts the user access. To manage the workload of the system, a scheduler is also put into use [15].Table 1 show the summary of various approaches used to prevent DDoS attacks.

Table 1: Summary of approaches against DDoS attacks in cloud

Techniques	Attributes	Restriction
Co-operative Intrusion Detection System	1.Avoids single point of failure attack 2.Improved reliability compared to pure Snort based IDS	Takes more computational time than pure Snort based IDS
Cloud Trace Back Model (CTB) and Cloud Protector	1.Averts direct DDoS with CTB 2.identity of attacker will be made known during successful DDoS attack	1. Collecting proper training data set for neural network is difficult. 2.Performance depends on accuracy of training data set
Confidence Based Filtering (CBF) Approach	Small storage size for nominal profile and high packet filtering efficiency, give better result than packet score.	Does not have high accuracy than other approaches. Applicable to network layer DDOS not for application layer.
CLASSIE Packet Marking Approach	1.Identifies HX-DoS attacks 2.Reduces false positive rate of DoS attacks	Helps to identify only application layer DDoS attacks.
Filtering Tree Approach	1.Uses double signature les to avoid XML rewriting attacks and client puzzles to detect HDoS attack 2.Filters attack in several stages	Can detect only application layers DDOS Attacks
Information Theory Based Metrics Method	1.uses the concept of entropy 2.Easy to implement and low false packet rejection rate	Chance of information loss due to aggregation in entropy
SOA based module	Detect application layers DDOS	Fails to detect network layer DDOS

IV. CONCLUSION

Cloud computing is world-changing wave of transformation. It is a next phase of internet that changes the way how internet is used by providing everything as a service on a pay per usage basis. Even though cloud offers a multitude of benefits to individuals and organizations, cloud is under high risk of attack and one such attack that can cause a major breach in security is DoS or DDoS attack. DDOS attack is easy to perform but defence to these can be complicated. The main difficulty with DDoS attack is that all the source addresses are spoofed so that it is not simple to find out the legitimate customer address i.e., so many addresses are unacceptable, therefore, it is not simple to filter actual customer address from these appeals. Numerous countermeasures had been approved and still developing for justifying against the DDoS attacks. Commonly DDoS attacks are influenced by an intruder trying to create an unlawful access in the target system's network. By prevention or detection of those attack standards of trust sharing become effective. This paper gives an idea of the various kinds of DoS attacks that can happen in a cloud and the various approaches that can be used to

protect the cloud to detect and prevent DDoS attacks. An ideal DDoS defence mechanism that deal with all ,must have some determined measures which includes Low False Positive Rate, Low Detection time, Low Negative rate, High Normal packet survival ratio. Exploration of precise approach for recognizing attacks and minimizing its after effect is a future research issue.

REFERENCES

[1] David R. Raymaon, Scott F. Midkiff "Denial-of –service in wireless sensor Networks: attack and defenses" IEEE CS, 2008.

[2] BhaskarParsadRimal, Eunmi Choi, Ian Lumb "A taxonomy and survey of cloud computing system" Fifth International joint Conference on INC,

[3] SameeraAbdulrahmanAlmulla, chanYeobYeun, "Cloud computing security management", IEEE, 2010.

[4] B. P. Rao, P. Saluia, N. Sharma, A. Mittal, and S. V. Sharma.Cloud computing for Internet of Things & sensing based applications. In Sensing Technology (ICST), 2012 Sixth International Conference on, pages 374–380. IEEE, 2012.

[5] G. Suciu, A. Vulpe, S. Halunga, O. Fratu, G. Todoran, and V. Suciu. Smart Cities Built on Resilient Cloud Computing and Secure Internet of Things. In Control Systems and Computer Science (CSCS), 2013 19th International Conference on, pages 513–518. IEEE, 2013.

[6] P. Kumar, S. Ranganath, W. Huang, K. Sengupta, Framework for real-time behavior interpretation from traffic video, IEEE Transactions on Intelligent Transportation Systems 6 (2005) 43–53.

[7] J. Gubbi, K. Krishna Kumar, R. Buyya, M. Palaniswami, Technical Report No. CLOUDS-TR-2012-2A, Cloud Computing and Distributed Systems Laboratory, the University of Melbourne, 2012.

[8] A. Gluhak, S. Krco, M. Nati, D. Pfisterer, N. Mitton, T. Razafindralambo, A survey on facilities for experimental Internet of Things research, IEEE Communications Magazine 49 (2011) 58–67.

[9] C. Vecchiola, R.N. Calheiros, D. Karunamoorthy, R. Buyya, Deadline-driven provisioning of resources for scientific applications in hybrid clouds with Aneka, Future Generation Computer Systems (2012) 58–65.

[10] Chi-Chun Lo, Chun-Chieh Huang, Joy Ku, A Cooperative Intrusion Detection System Framework for Cloud Computing Networks, 39th IEEE International Conference on Parallel Processing Workshops, 2010, pp280-284./

[11] Bansidhar Joshi, A. SanthanaVijayan, Bineet Kumar Joshi, Securing Cloud Computing Environment Against DDoS Attacks, IEEE International Conference on Computer Communication and Informatics, 2012.

[12] Qi Chen, Wenmin Lin, Wanchun Dou, Shui Yu, CBF: A Packet Filtering Method for DDoS Attack Defense in Cloud Environment, Ninth IEEE International Conference on Dependable, Autonomic and Secure Computing, 2011.

[13] E.Anitha, Dr.S.Malliga, A Packet Marking Approach to Protect Cloud Environment against DDoS Attacks, International Conference on Information Communication and Embedded Systems, 2013.

[14] TarunKarnwal, T.Sivakumar, G.Aghila, A Comber Approach to Protect Cloud Computing against XML DDoS and HTTP DDoS attack, IEEE Students' Conference on Electrical, Electronics and Computer Science, 2012, vol-01, pp-9-12.

[15] S. Renuka Devi and P. Yogesh, Detection Of Application Layer DDos Attacks Using Information Theory Based Metrics, CS & IT-CSCP 2012, pp.217–223.

[16] K. Kumar, A. L. Sangal, and A. Bhandari, "Traceback Techniques Against DDoS Attacks: A Comprehensive Review," Proc. of 2nd Intl' Conference On Computer and Communication Technology (ICCCT), IEEE, pp. 491-498, September 2011

[17] H. Beitollahi, and G. Deconinck, "Denial of Service Attacks: A Tutorial,", Electrical Engineering Department (ESAT), University of Leuven, Technical Report: 08-2011-0115, August 2011.

[18] Marwan Darwish, Abdelkader Ouda, Luiz Fernando Capretz: Formal Analysis of an Authentication Protocol against External Cloud-Based Denial-of-Service (DoS) Attack.

[19] Trends in Denial of Service Attack Technology CERT® Coordination Center Kevin J. Houle, CERT/CC George M. Weaver, CERT/CC In collaboration with: Neil Long Rob Thomas v1.0 October 2001.

[20] P. Ferguson, and D. Senie, "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing," RFC 2827, May 2000.

[21] http://dazeinfo.com/2015/08/28/internet-security-ddos-attacks-china-australia-us-uk-akamai/.

