International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Identification and Avoidance of DDoS Attack for Secured Data Communicationin Cloud

Aaqib Iqbal Wani[1], Janaki Raman V.[2], N. Priya[3]

[1, 2]B.Tech Computer Science and Engineering, Bharath University

[3]M. Tech Computer Science and Engineering, Assistant Professor, Bharath University

Abstract: ***Cloud is turning into a prevalent computing platform. Certainly, a question arises on the off chance that we can crush the scandalous DDoS attacks in a cloud environment. A DDoS attack can collapse the whole system in a Cloud Server environment, however in case of cloud it is not that powerful but still to some extend disturbs the normal activity of the system. At the point when a DDoS attack occurs in a client environment, we devote the idle resources of the cloud to clone adequate Intrusion Prevention Systems for the exploited client in order to rapidly channel out attack packets and ensure the QoS (Quality of Service) for benign users simultaneously. In the proposed model we deploy multiple Intrusion Prevention System (IPS) to screen client activity and filter the requests in light of the conduct and forward to the corresponding servers through cloud server. Each server would have certain space designated in the cloud server. The IPS's continually monitor the activity of the users to counteract DDoS attacks.***

Keywords: Cloud computing, DDoS attacks, DynamicResource allocation, System Modelling

1. Introduction

In this paper, we demonstrate one of the approaches to identify and avoid DDoS attacks in a cloud environment. A key issue of a DDoS attack and defence is resource competition. If a defender has adequate resources, the attack will be unsuccessful and vice versa. A cloud infrastructure provider pools large amount of resources and makes them easily accessible in order to handle a fast increment in service demands [1]. Therefore, it is nearly impossible for a DDoS attack to shut-down a cloud. However, the Client Server and the P2P platforms, do not possess adequate resources to confront DDoS attacks.

The individual cloud customers (referred to as parties hosting their services in a cloud) cannot get away from DDoS attacks as they do not have the advantage. It is very much likely for an individual cloud customers to win the battle by benefiting from the unique features of clouds. In this paper, we explore a way to tackle DDoS attacks against individual cloud customers from the resource competition view point. Regardless of the guaranteeing plan of action and reputation encompassing cloud computing, security still remains a significant sympathy toward organizations moving their applications to cloud [2], [3].

Distributed Denial of Service (DDoS) attack is one of the significant dangers for non-cloud computing environments, such as E-commerce Websites, Independent News Websites and Online Games [4]. DDoS attacks are accomplished with the assistance of botnets. Resent investigations [5] have rectified the conviction that hackers can easily compromise computers at whatever time they need. However, due to anti-viruses and anti-malwares, the number of active bots a botmaster can manipulate has been compelled to hundreds or few thousands level.

In the early works DDoS attacks were dealt as a resource management problem. Recent studies [6], [7], [8] have exhibited that the key issue of DDoS attack and defence is a competition for resources and evidently the winner is the side who possesses more resources. Unlike other computing platforms, a cloud environment usually has large amount of resources, full control, and dynamic allocation capability of resources. Hence, it is impossible to deny the services of a cloud with the scale of current botnets.

Cloud service providers (CPS) generally offer cloud clients two resource provisioning plans: "Short-Term on Demand" and "Long-Term Reservation" plan. In the "Short-Term on Demand" plan, the customer will be charged in light of what he utilizes. This resource business model can easily be compromised by an Economic Denial of Sustainability (EDoS) [10], [11] attack. Also, this kind of attack can disturb the service of cloud that allocates resources based on spot instance [12], [13]. On the other hand, in case of "Long-Term Reservation" plan, the customer will typically make the source reservation for the most extreme utilization of his business. In other words, the reserved resource for his application are confined, in that capacity risk of DDoS attack remains.

As a new business model and computing platform, plenty of research is being done on cloud, such as economical modelling [14] and resource optimization [15]. In any case, experimentation on DDoS attacks and defence in a cloud environment is still in the early stages. The available cloud security covers various facets, such as attack mitigation techniques against DDoS attacks [16] or EDoS attacks [11], DDoS defence as a cloud service [17], and security architecture against DDoS attacks in cloud computing [18].

In this paper, we propose a practical dynamic resource allocation mechanism to dodge DDoS attacks that targets individual cloud clients. Generally, there is one or several access points between a cloud data centre and the internet. We place our Intrusion Prevention System (IPS) at these points to screen the incoming packets. As soon as the cloud hosted server comes under a DDoS attack, the proposed mechanism will automatically and dynamically allocate extra resources from the available cloud resource pool, and

will clone new virtual machines based on the image file of the original IPS using the existing clone technology [19], [20]. All the IPS's will cooperate together to filter attack packets out, and ensure the quality of service (QoS) for benign users. As soon as the volume of DDoS attack packets declines, the proposed mitigation system will automatically reduce the number of IPS's, and release the extra resources back to the cloud resource pool.

It has to be noted that the objective for this paper is to explore the possibility of identifying and avoiding DDoS attacks in a cloud environment from a technical and resource competition point of view. Therefore specific DDoS detection methods are not included neither are the business issues which may be caused by our mitigation proposal. With the utilization of the proposed system, we believe most DDoS attacks can be defeated. This will to some extend make cloud customers more persuaded in moving their businesses to cloud platforms. The commitments of this paper are as per the following:

- We point out that DDoS attacks do possess a security risk for individual cloud customers. On the other hand by exploiting the cloud platform, DDoS attacks can be prevented.
- We propose a dynamic resource allocation mechanism to automatically deal with the available resources of a cloud to diminish DDoS attacks on individual cloud clients. The proposed method exploits the dynamic resource allocation feature of cloud platforms, and is quite simple to implement.
- We demonstrate a queuing theory based model to assess the resource allocation against different attack qualities. Real-world data based analysis and investigation help us to infer that it is conceivable to defeat DDoS attacks in a cloud domaininside moderate costs.

2. DDOS Attack Mitigation in Clouds

In this segment, we put forward a mechanism to dynamically allocate extra resources to an individual cloud hosted server when it comes under DDoS attack. Above all else the features of a cloud hosted virtualserver are examined in a non-attack scenario. As demonstrated in Fig. 1a, a cloudhosted service includes a server, an intrusion prevention system (IPS in the diagram), and a buffer for packets (queue Q in the diagram). All the packets from benign users go through the queue, pass the IPS and are then responded by the server. As such, the number of benign users is stable, and we presume the virtual IPS and virtual server have been allocated sufficient resources, and accordinglythe quality of service (QoS) has been provided.

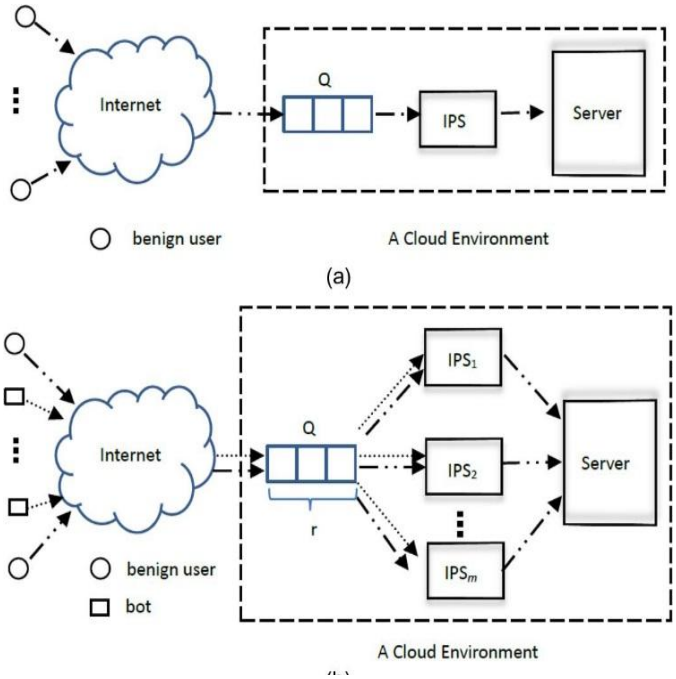

Figure 1: (a) Cloud hosted server in a non-attack situation (b) Cloud hosted server under DDoS attack with the mitigation strategy set up

At the point when the hosted virtual server is under a DDoS attack, countless attack packets are generated by botnets, and pushed to queue Q. In order to identify the attack packets and guarantee the QoS to benign users, we require more resources to clone multiple IPSs to complete the task. We intend to clone multiple parallel IPS's to accomplish the task as shown in Fig. 1b. The number of IPS's required to achieve this objective is dependent on the magnitude of the attack packets. As discussed earlier, the attack capability of a botnet is usually restricted, and the required amount of resources to confront the attack is not very large. In general, it is sensible to expect that a cloud can deal with its reserved or idle resources to take care of the demand.

3. System Analysis and Modelling

In this segment, we first discuss the existing and the proposed system `for moderating a DDoS attack on a cloud. Then we discuss the modules required to model the system in general, and then establish an executable model to successfully identify and avoid a DDoS attack in a cloud environment.

3.1.1 Existing System

DDoS attack in a client server environment would collapse the entire system, but as much as cloud is concerned it may not be that effective but still will try to disturb the regular activity of the system.

Disadvantage:
1. Lack of a Proper Security System.
2. Single IPS is used for Intrusion Detection.
3. The activity of users is not monitored properly.

3.1.2Proposed System

We deploy multiple Intrusion Prevention System (IPS) in order to monitor the activity of the users and filter the

requests based on the behaviour and forwards to the corresponding servers through cloud server. Every server allocates certain space in cloud server. IPS monitors the activity of the users to avoid DDoS attacks. In the modification, few DDoS attacks are listed and monitored. The user behaviour patterns are 1. Continuous & same request from single user in a given period of time, 2. Distinctive queries from the same user within a given period of time, 3. Diverse queries from distinctive users but from same IP, 4. Request of file size beyond the permitted limit. Based on these patterns user behaviour is monitored and DDoS attack avoided.

Advantage
1. Multiple IPS'sare deployed.
2. DDoS attack can be identified.
3. Performance is increased due to blocking of DDoS attack.

3.2 Modules

The following modules are required in order to make our modelling and analysis feasible and practical: The sequence diagram is showed at the end of the section.
1. Cloud Server Deployment
2. Space Allocation
3. User Mustering
4. Deployment of Multiple IPS
5. DDOS from Single User
6. DDOS from Multiple User from same IP
7. Attacks Filtering Model

3.2.1 Cloud Server Deployment
Cloud Service Provider will contain the large amount of data in their Data Storage Centre. . The User information is stored in the Cloud Service Provider's database The Cloud Service provider will also maintain all the User information to authenticate the user when the user tries to login to their account. Also, the Cloud Server will redirect the User requested job to the Resource Assigning module to process the requested job. The resource assigning module will process the request of all the users. To communicate with the client and with the other modules of the cloud network, the cloud serverestablishes a connection between them. For this purpose we will create a user interface frame. The cloud service provider will send the user job request to the resource assign module in Fist in First out (FIFO) manner.

3.2.2 Space Allocation
Cloud Server is a cloud infrastructure service that permits users to deploy hundreds of cloud servers instantly and create advanced and high availability architectures.A Cloud Server is typicallya virtual machine running on a hypervisor for Linux-based instances, and XenServer for Windows and Linux instances. Each quad core hardware node comprises between 16 GB to 32 GB of RAM andpermitting distributions between 256 MB to 30 GB. Disk and CPU allocations scale up with memory, the disk sizes range from 10 GB to 620 GB. Many Linux distributions are supported.

3.2.3 User Mustering
In this module we tell about the user mustering in which we can:
1. Track Users during an Emergency.
2. Ensure nobody is left in danger zone.
3. Reduce Paperwork / Human Error.
4. Data collection and reporting.
5. Get workers back into facility in a safe and timely manner.

3.2.4 Deployment of Multiple IPS
In this module we employ multiple IPS'si.e. Intrusion Prevention System that are used to protect the user from DDoS attacks. In the existing system single IPS is used to scan the query of a cloud user. But in the proposed system we deploy multiple IPS to monitor the user query so that it easily defends the attack.

3.2.5 DDoS from Single User
DDoS is a type of Denial of Service (DOS) attack in which multiple compromised systems are utilized to target a single system causing a Denial of Service (DoS) attack. The DDoS attack consists of both the end targeted system and all other systems maliciously used and controlled by the hacker. The incoming traffic flooding the victim originates from wide range of sources – potentially hundreds of thousands or even more compromised systems. It in this manner becomes impossible to avoid the attack simply by blocking a single IP address and significantly more hard to recognize between genuine user traffic and attack traffic when spread across distinctive sources.

3.2.6 DDoS from Multiple User from Same IP
To launch a DDoS attack, hackers first build a network of computers that consists of a large number of compromised hosts. In the existing system multiple users will be logged in from the same IP address and send query. The existing system consists of a single IPS that is not capable of monitoring multiple users and thus leads to an overload on the server. In our proposed model we detect DDoS attacks by monitoring the query coming from multiple users from the same IP address in a given period of time.

3.2.7 Attacks Filtering Model
We put forward a (PPF) Probabilistic Packet Filtering mechanism of action to protect the Web server against Distributed Denial-of-Service (DDoS) attacks. In the attack filtering model we implement the requested huge sized file beyond the permitted limit. By monitoring these user behaviour patterns, DDoS attack is avoided in cloud.

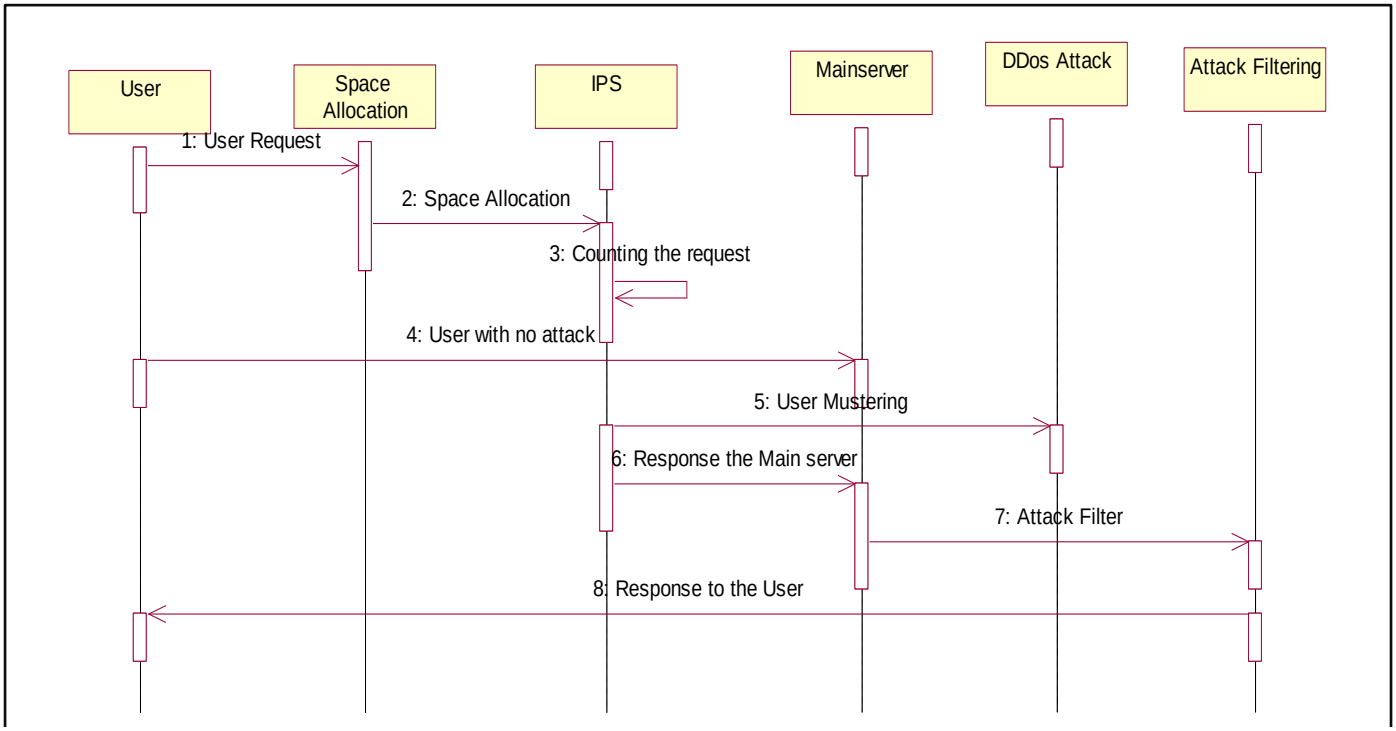

Figure 2.3: Sequence Diagram

4. Feasibility Study

In this phase we analyse the feasibility of the project and a business proposal is put forward with a general plan for the project and some approximate cost estimates. The feasibility study of the proposed system is to be carried out during system analysis. This is done in order to ensure that the proposed system is not a burden to the company. For feasibility analysis, understanding of the major requirements for the system is necessary.

4.1 Economical Feasibility

The Economic Feasibility study is carried out in order to check the economic impact that the system will have on the organization. The amount of funds that the company can invest in the research and development of such a system is limited. Consequently, the developed system ought to be well inside the monetary allowance and this was effectively accomplished because most of the technologies used are free and easily available. However, the customized products had to be purchased separately.

4.2 Technical Feasibility

The Technical Feasibility study is carried out in order to examine the technical requirements of the system. The developed system must not exhibit a high demand on the available technical resources. This will eventually lead to high demands being placed on the client. As such, the developed system must require modest requirements.

4.3 Social Feasibility

The part of Social Feasibility study is to test the level of approval of the system by the user. It incorporates the procedure of training the user to operate the system efficiently. The user must not feel isolated by the system, instead accept it as a necessity.

5. Conclusion

In this paper, we point out that DDoS attacks are still an effective tool for cyber criminals to shut down individual cloud customers, even though it is almost impossible to deny the service of a cloud platform. At the same time, we also note that a cloud possesses a potential to counter this kind of brute force attack by using its profound resources. Motivated by this, we design a strategy to dynamically allocate idle or reserved cloud resources to those cloud customers who are experiencing DDoS attacks in order to defeat the attacks, and at the same time guaranteeing the quality of service for benign users. We establish a queuing theory based model for the proposed DDoS attack mitigation scheme in a cloud environment. Real-world data set based experiments and simulations confirm our claim that we can beat DDoS attacks on individual cloud hosted services with an affordable cost to cloud customers.

As a rarely explored new area of research, there is plenty of work expected to be completed in the near future. As future work, we want to explore what should we do if a cloud data centre runs out of resources during a battle. Secondly, we would like to discover whether it is possible for attackers to rent the resources of a cloud to carry out their attacks on servers hosted by the same or other clouds. Finally, real cloud environment tests for the proposed method are expected in the near future.

References

[1] M.Armbrust,A.Fox,R.Griffith,A.D.Joseph,R.H.Katz,A. Konwinski,G.Lee,D.A.Patterson,A.Rabkin,I.Stoica,and M.Zaharia, ‘‘Abovethe clouds: A Berkeley view of

cloud computing,'' EECS Dept.,Univ.California, Berkeley,CA, USA, Tech. Rep.UCB/EECS-2009-28, Feb. 2009.
[2] S. Subashini and V. Kavitha, ''A Survey on Security Issues inService Delivery Models of Cloud Computing,'' J. Netw. Comput. Appl., vol. 34, no. 1, pp. 1-11, Jan. 2011.
[3] R. Bhadauria, R. Chaki, N. Chaki, and S. Sanyal, ''A Survey on Security Issues in Cloud Computing,'' CoRR, vol. abs/1109.5388, 2011.
[4] T. Peng, C. Leckie, and K. Ramamohanarao, ''Survey of Network-Based Defense Mechanisms Countering the dos andDDoS Problems,'' ACM Comput. Surv., vol. 39, no. 1, pp. 1-3, 2007.
[5] M.A. Rajab, J. Zarfoss, F. Monrose, and A. Terzis, ''My Botnetis Bigger Than Yours (Maybe, Better Than Yours): Why SizeEstimates Remain Challenging,'' in Proc. 1st Conf. HotBots, 2007, p. 5.
[6] S. Yu, S. Guo, and I. Stojmenovic, ''Can We Beat LegitimateCyber Behavior Mimicking Attacks from Botnets?'' in Proc.INFOCOM, 2012, pp. 2851-2855.
[7] Y. Chen, K. Hwang, and W.-S. Ku, ''Collaborative Detection ofDDoS Attacks over Multiple Network Domains,'' IEEE Trans. Parallel Distrib. Syst., vol. 18, no. 12, pp. 1649-1662, Dec. 2007.
[8] J. Francois, I. Aib, and R. Boutaba, ''Firecol, a CollaborativeProtection Network for the Detection of Flooding DDoS Attacks,''IEEE/ACM Trans. Netw., vol. 20, no. 6, pp. 1828-1841, Dec. 2012.
[9] S. Chaisiri, B.-S. Lee, and D. Niyato, ''Optimization of ResourceProvisioning Cost in Cloud Computing,'' IEEE Trans. Serv. Comput., vol. 5, no. 2, pp. 164-177, Apr./June 2012.
[10] J. Idziorek, M. Tannian, and D. Jacobson, ''Insecurity of CloudUtility Models,'' IT Prof., vol. 15, no. 2, pp. 22-27, Mar. /Apr. 2012.
[11] M.H. Sqalli, F. Al-Haidari, and K. Salah, ''Edos-Shield-a Two-Steps Mitigation Technique against Edos Attacks in CloudComputing,'' in Proc. UCC, 2011, pp. 49-56.
[12] Q. Wang, K. Ren, and X. Meng, ''When Cloud Meets Ebay:Towards Effective Pricing for Cloud Computing,'' in Proc.INFOCOM, Mar. 2012, pp. 936-944.
[13] S. Yi, A. Andrzejak, and D. Kondo, ''Monetary Cost-AwareCheckpointing and Migration onAmazon Cloud Spot Instances,''IEEE Trans. Serv. Comput., vol. 5, no. 4, pp. 512-524, Fourth Quarter 2012.
[14] J. Cao, K. Hwang, K. Li, and A. Zomaya, ''Optimal MultiserverConfiguration for Profit Maximization in Cloud Computing,''IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 6, pp. 1087-1096, June 2012.
[15] H. Wang, F. Wang, J. Liu, and J. Groen, ''Measurement andUtilization of Customer-Provided Resources for Cloud Computing,''in Proc. INFOCOM, 2012, pp. 442-450.
[16] R. Lua and K.C. Yow, ''Mitigating DDoS Attackswith Transparentand Intelligent Fast-Flux Swarm Network,'' IEEE Netw., vol. 25,no. 4, pp. 28-33, July/Aug. 2011.
[17] P. Du and A. Nakao, ''Ddos Defense as a Network Service,'' inProc. NOMS, 2010, pp. 894-897.
[18] J. Chen, Y. Wang, and X. Wang, ''On-Demand Security Architecturefor Cloud Computing,'' Computer, vol. 45, no. 7, pp. 73-78, July 2012.
[19] R.Wartel, T. Cass, B. Moreira, E. Roche, M. Guijarro, S.Goasguen,and U. Schwickerath, ''Image Distribution Mechanisms in Large Scale Cloud Providers,'' in Proc. CloudCom, 2010, pp. 112-117.
[20] J. Zhu, Z. Jiang, and Z. Xiao, ''Twinkle: A Fast ResourceProvisioning Mechanism for Internet Services,'' in Proc. INFOCOM,2011, pp. 802-810.