ISSN 2250-3153

A PREVENTION OF DDOS ATTACKS IN CLOUD USING NEIF TECHNIQUES

***J.RAMESHBABU, *B.SAM BALAJI, *R.WESLEY DANIEL,**K.MALATHI**

*PG STUDENTS

**ASSISTANT PROFESSOR

Department Of Computer Science and Engineering
Saveetha School of Engineering, Saveetha University, Chennai

Rameshbabu18.j@gmail.com
Sambalajibj06@gmail.com
Leydaniel07@gmail.com
Malathi.infotech@gmail.com

Abstract: In recent years, most of the organizations in the world have increasingly realized the importance of cloud platforms. The cloud computing is one of the developing segmenting of IT industry as well as a promising concept to the end users. However Cloud Computing has more applications but there are many challenges that are facing by a Cloud environment. In recent years, the major attacks in cloud are a Distributed denial of service (DDoS) attacks on the catalog of cloud attacks. DDoS can have serious penalty for the companies which are dependent on the internet service for their production. Thus, it is important to reduce a force of DDoS is one of the latest issues. This paper focus on the impact of DDoS attacks in cloud and the NEIF technique available to overcome with the issue.

Keywords: Cloud Security, Distributed Denial of Service(DDoS), Egress and Ingress filtering.

1. INTRODUCTION

Cloud Computing, is the fastest developing field of IT industries. Cloud Computing is an Internet based computing where implicit shared servers provides all needed resources such as software, hardware, platform, Infrastructure, devices to the Cloud users[2]. The main advantage of the Cloud Computing is that the customer

Can able to select their required resources and pays only for what they use and how much time they were using that resources. Now a day large amount of information about persons and organizations are kept in the Cloud, so obviously questions will rise regarding the security and privacy of the Cloud environment. There is still unwillingness among the Individuals and companies to accept a Cloud environment due to lack of security and privacy mechanisms. Security problems play a vital role in slowing down the acceptance of Cloud environment among the users and companies. According to the two surveys done by an International data Corporation (IDC) [1] in 2008 and 2009 respectively, security is top most issue in a Cloud environment. Although Cloud service provider provides some traditional security mechanisms still there are more non-identifiable attacks have been launched against the Cloud environment. One such attack is Distributed Denial of Service (DDoS) attack. In recent years there are significant number of attacks have been launched against a Cloud environment, so it is necessary to take steps against defending DDoS attack in Cloud environment. The purpose Denial of Service attack is to make the network resources such as internet, web services and applications unavailable to the genuine users for a certain period of time [6]. A Distributed Denial of Service (DDoS) attack is a synchronized attack that is performed by compromising less important systems to launch an attack against a target system or network [6]. On February 9, 2000 there are more number of DDoS attacks are performed against various websites such as against Yahoo.com, Amazon, eBay.com, E*Trade, Buy.com FBI and more websites fell wounded to DDoS attacks resulting in a huge amount of damage and difficulty [Garber 2000] [7]. In 2004, chain of DDoS attacks launched against several of companies which providing anti-spam services. These attacks make companies services inoperable for large period of time. Hence it is necessary to defend and mitigate a DDoS attack to minimize the damages to Cloud environment.

This paper proposes an innovative implementation of DDoS defense technique named Network Egress and Ingress Filtering (NEIF), which can be implemented at ISPs' edge routers, to avoid a DDoS attacks in Cloud. With NEIF technique, an Internet Service Provider (ISP) can easily protect their clients against a DDoS attack (egress Filtering), but also protect their networks from participating in spreading DDoS attacks (ingress filtering). NEIF can work as an enhancement of the on hand network ingress filtering (RFC2827) [9]. Spoofer Project [10] shows that already 80% ISPs have implemented an RFC2827 to protect against an IP spoofing attack NEIF technique is easy to implement and it is transparent to the client side, so it can be easily accepted by all Internet Service Providers (ISPs).

2. DISTRIBUTED DENIAL OF SERVICE

Synchronized attack on the availability of services of a given victim or network that is launched indirectly through many compromised systems. The DDoS attacks are performed by three

main units: (1) Master: Master is the attacker who launches the attack indirectly through a series of compromised systems. (2) Slave: The compromised system which is used to launch an attack is known as Slave. (3)Victims: The system which undergoes an attack launched by an attacker is known as Victim. There are two types of victims. Systems which are under attack are referred to as "primary victim", and the systems which are compromised to launch an attack are referred to as "secondary victims." DDoS attack normally occurs in two phases. First phase is an interruption Phase. During this stage the Master tries to compromise less important system to perform a DDoS attack by flooding a large number of requests to a target system. The second stage involves installing a DDoS tools to attack a target system.

3. CLOUD COMPUTING

Cloud Computing is getting widespread in the business and IT industry. Clouds Computing can be defined as an Internet based computing where Virtual shared servers provide all the required resources to the Cloud customer [2]. The main advantage of Cloud Computing is that the customers can able to select what they want and at any location. It also aims to reduce the maintenance cost and operational cost. The third party provider commonly known as Cloud provider provides all physical infrastructure for rent so Cloud customer need not to own the physical infrastructure, thus reduces the cost of physical infrastructure.

There are three layers in the Cloud computing these three layers are discussed below:

A. Cloud Application

This is the first layer of the Cloud. The remote client will access all applications and data provided by a web browser. So there is no need for installing the application on customer's computer and there by it reduces the maintenances cost and operational cost of a Companies.

B. Cloud Platform

This is the second layer in the Cloud. The computational service is provided by this layer to the customer. This Computational service enables customers to make changes in the server's configuration and settings according to the demand of a customer.

C. Cloud Infrastructure

The third and last most layer of the Cloud provides a Cloud Infrastructure. The concept of Virtualization is provided by this Cloud layer. Virtualization enables customers to share various software and hardware components and provide platform by means of splitting a single piece of hardware and independent components. Virtualization is the creation of a near version of software and hardware components. These are then interconnected with others for flexibility and additional storage [3].

The cloud computing layers are described in architecture diagram as following:

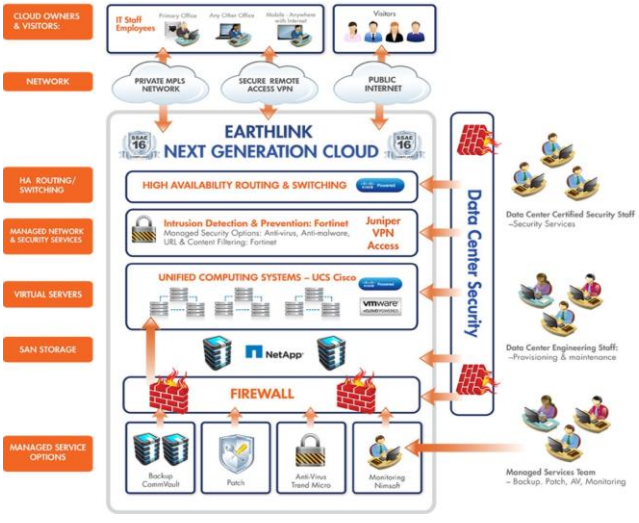

Figure 1: Cloud Architecture

The main benefits for all the small scale and large scale organizations using Cloud Computing is mentioned below,

A. Reduction of Cost

By shifting to Cloud environment Customers can avoid heavy expenditure of spending large amount of cost for establishing set-up. This also reduces the operational cost. The customer pays for only what they use.

B. Scalable and Flexible

Companies can able to start business from simpler model and can then go for the complex model and if required can again come back to the simpler model. Flexibility enables Customers to use more resources at peak time in order to satisfy the requirements of client.

C. Quick and Easy Implementation

A Company can get the Cloud service in short period of time and easy to implement without any software licenses or implementation services.

D. Reduced Maintenance Cost

The Cloud service provider provides all maintenances to the customer and maintenance of application is done by APIs, thus reducing maintenance cost.

E. Quality of Service

Cloud service provider provides 24*7 support and immediate service in case of faults.

F. Mobility

Cloud customer can able to access the data and application from any location at any time by just having an internet connection. So it is idle for increasing productivity by a mobile user.

4. CHALLENGES OF CLOUD COMPUTING

Cloud Computing have lots of challenges. These challenges are discussed as follows:

A. Security and Privacy

The security is a main concern for a cloud computing. Customers are still not comfortable in keeping all data about companies in a cloud because of vulnerability from various places. Since Cloud is accessed by various persons the next challenge of cloud is Privacy. So it is important to ensure costumer that the confidential information are not accessed by any other users by a Cloud service provider.

B. Lack of Standards

There are no proper standards have been followed in a cloud environment, so it is necessary to provide a proper standard.

C. Loss of Control

The important issue in cloud environment is that the data may be lost when the person is not using it for a period of time. So providing a control of data to the user is a important work by an Cloud service provider.

5. DDOS ATTACKS IN CLOUD

In early 2000, a series of DDoS attacks were launched against a more critical websites such as Yahoo.com, Amazon and E Trade. On May 2001 a huge amount of attacks were performed on grc.com. During that time the internet is helpless against a destructive DDoS attacks. The successful DDoS attack makes a huge impact on the organization which depends on the internet for their production. Based on the survey between 1989 and 1995, 51% of attacks filled a disk, 33% of attacks degraded the network performance and 26% of attacks destroy files which containing the Real DoS incidents in the Internet between the years 1989 and 1995 were investigated. The three most typical effects were the following: 51% of these incidents filled a disk, 33% of the incidents degraded network service, and 26% of the incidents deleted some file containing important data.. On august 1999, a vigorous DDoS attacks has been launched against a university. This incident makes university network to shut down for two days. 1 Gbit/s of traffic can be produced by a DDoS attacks against a target system or network. The impact of DDoS attack on internet can be measured by a backscatter analysis. On May 2001, The Coordination Center of the Computer Emergency Response Team (CERT) has been attacked by a DDoS attack. The main target for DDoS attack is a Domain Name System (DNS). The DDos attack causes a huge amount of traffic so that DNS requests cannot be able to reach a root name server. On June 15, 2004 against name servers on Akamai's Content Distribution Network (CDN), has been attacked by a DDoS attack. On January, 2005 DDoS attack make to shut down the Internet-based business service of Al Jazeera. According to backscatter analysis nearly 2000-3000 active have been launched per week. In a period of three years, nearly 68,700 attacks have been launched against various internet sources. The Table 1 lists some of the recent DDoS attacks incidents.

6. NEIF TECHNIQUES

NEIF installed at the ISPs' edge routers and plays as a dual role in shielding DDoS attacks. As a first role, the goal of ingress filtering is to discover and prevent the DDoS attacks launched from its customers. Actually, the ingress filtering has already been extensively deploying to avoid source IP spoofing by discarding packets which have a source address which is not allocated to that customer. Our proposed ingress filtering can be a supplement of the existing one. Ingress filtering can ensure an ISP's network do not participate in flooding DDoS attacks. Ingress filtering requires the understanding between Internet Service Providers (ISP's) so it takes more amount of time to implement at all ISP's. Egress filtering is used to protect ISP's customers from being attacked. Note that single egress filtering cannot avoid major flooding attack that may damage the Internet infrastructure directly. However, if most ISPs have already deployed ingress filtering, egress filtering can work well. Network filtering can operate either on traffic aggregates (ACC-Pushback [13] and MULTOPS [11]) or on individual flows (D-WARD [12] and RED-PD [14]). According to [15], due to lack of infrastructure capabilities for enabling large numbers of packet filters for all flows, many ISPs still implement aggregate-based filtering that discards all packets to a victim at ingress to minimize guarantee damage to the infrastructure. Since flow-level filtering can directly tell how a flow should be coordinated. However, a main obstacle to execute flow-level filtering is that it is infeasible to exactly compute all flows. Additionally keeping a counter costs more for each flow, since it grows linearly with the number of flows even with state-of-the-art sampling technique such as Cisco Net Flow [16].

Egress filtering is used to filter the networks outbound traffic. Why is this significant? Either through malicious intent or simple misconfiguration of a network, sites can flood the Internet with bogus packets. On February, 2000 the sites are hacked exclusively to send bogus packets to other servers on the network. Traditionally, the traffic can be filtered by routers and firewalls but these strategies will leave the Distributed Denial of Service (DDOS). Egress filtering can be able to detect and prevent the Distributed Denial of Service (DDOS) attacks. DDOS attacks can be controlled by implementing egress filtering at the networks.

This paper briefly converse the benefits of egress filtering, gives examples for what common DDOS tools it can block, and directs the reader to sites with specific details on how to execute this filtering at the site. The egress filtering is used to prevent packets with invalid or incorrect address leaving form the system. These invalid packets may be originate from a misconfigured router in network or, more dangerously, from a compromised system hosting one of the many DDOS tools available. Egress filtering usually occurs at the edge of a network, at the firewalls and border routers. At no time should the network send out any packets with addresses not legally assigned to you – to do so means either firewall may be misconfigured to show the world how internal address space, or worse, that you are the home of one or more DDOS attack agents. There should be very little effect or loss of functionality to the network when implementing egress filtering – all justifiable traffic requires is in legal addresses, so blocking anything else will only break things that should not be sent in the first place! The firewalls and routers struggle to prevent the

traffic, when the site has been already compromised.. Similar to egress filtering, Ingress filtering is the filtering of "any IP packets with untrusted source addresses before they enters and affect the system" This can be implemented at ISP level where it can be cleanly hold_the packets coming through their many networks. Unfortunately, for some of the larger ISP's like AT&T and sprintlink.net, they connect such a huge quantity of networks that filtering for legal addresses is tremendously complicated. Ingress filtering has its limitations – for large ISP's, other companies with different addresses may be using their backbone. To prevent those addresses from going through the network would be its own form of denial of service attack. Keeping track of the many genuine addresses that can go through a large ISP is next to impossible – it is better to have security as close to the source as possible, encouraging each site to perform their own egress filtering.

The architecture of the NIEF and Edge routers at ISP's are shown in figure below,

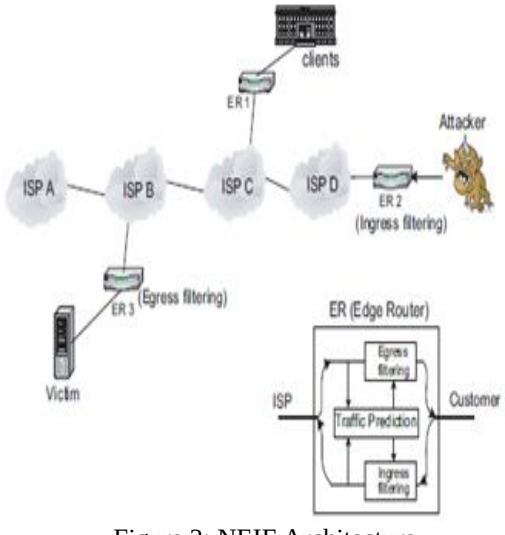

Figure 2: NEIF Architecture

By implementing NEIF Technique at ISP's edge routers we can improve the throughput. The graph in figure 3 shows the throughput of the victim under various deployment models.

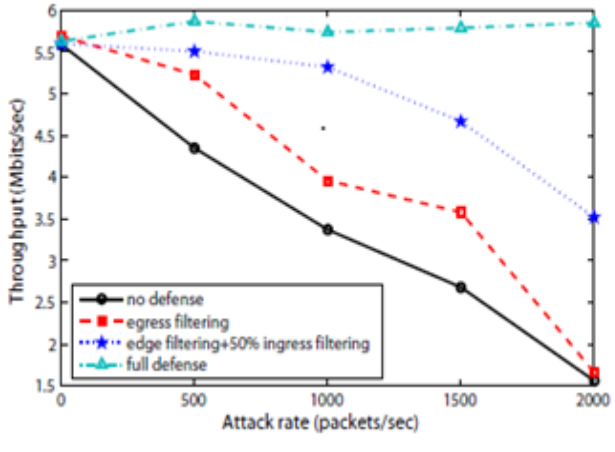

Figure 3: THROUGHT OF VICITM

As well as the connection delay has been reduced by deploying NEIF Technique at ISP's edge routers. The graph in figure 4 shows the average connection delay under different deployment models.

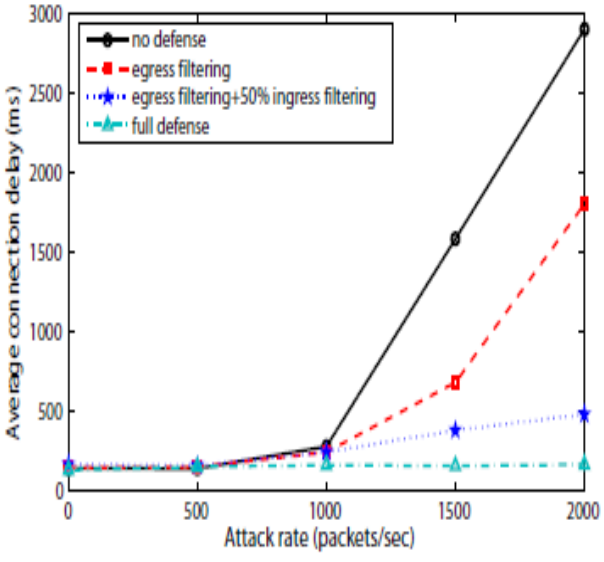

Figure 4: REDUCITON OF CONNECTION DELAY

7. CONCLUSION AND FUTURE ENHANCEMENT

This paper summarizes a challenges of cloud computing and the impact of DDoS attack in Cloud environment. This paper proposes network egress and ingress filtering, called NEIF technique to defensive method against DDoS attack. Through NEIF technique it is easy to detect and mitigate DDoS attacks. NEIF technique can be implemented with less complexity and it is translucent to the client-side So that it can be easily accepted by Internet Service Providers (ISPs). In future the NEIF performance can be improved by implementing NetFPGA. Egress filtering, enables to works around the attacker so it is easy to trace back the compromising system and makes attacker difficult to launch an attack against a target system. If NEIF technique is implemented at all ISP's routers it is easy to defend and mitigate a DDoS attack in cloud platform

REFERENCE

[1] http://www.in.idc.asia/ (accessed in Feb, 2013)
[2] "Luit Infotech: What is Cloud Computing", Download,pp1http://www.luitinfotech.com/kc/what-is-cloud-computing.pdf (accessed in Feb 2013)
[3]http://searchservervirtualization.techtarget.com/definition/virtualization (accessed in Feb 2013)
[4]http://searchcloudcomputing.techtarget.com/definition/cloud-computing (accessed in Feb 2013)
[5] Martin Roesch," SNORT — Lightweight Intrusion Detection for Networks", In *Proceedings of LISA '99: 13th Systems Administration Conference*, pp. 229-238, November 7–12, 1999
[6] Stephen M. Specht, Ruby B. Lee," Distributed Denial of Service: Taxonomies of Attacks, Tools and Countermeasures". In Proceedings of the 17th International Conference on Parallel and Distributed Computing Systems,2004 International Workshop on Security in Parallel and Distributed Systems, pp. 543-550, September 2004.
[7] Tao Peng , Christopher Leckie, Kotagiri Ramamohanarao, 'Survey of Network-based Defense Mechanisms Countering the DoS and DDoS Problems",

ACM Transactions on Computational Logic, Vol. 2, No. 3, Pages 1-0??.. 09 2006
[8] Radwane Saad, Farid Nait-Abdesselam and Ahmed Serhrouchni, "A Collaborative Peer-to-Peer Architecture to Defend Against DDoS Attacks". In *33rd IEEE conference on local computer network*, pp. 427- 434, IEEE, September 2008
[9] Sebastian Roshke, Feng Cheng, Christoph Meinel, "Intrusion Detection in the Cloud". In *Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing*, pp. - 729-734, IEEE, October 2009
[10]"Spoofer project," http://spoofer.csail.mit.edu/.
[11] T. M. Gil and M. Poletter, "Multops: a data-structure for bandwidth attack detection," in *USENIX Security*, 2001.
[12] J. Mirkovic, G. Prier, and P. Reiher, "Attacking ddos at the source," in *ICNP*, 2002.
[13] R. Mahajan, S. M. Bellovin, S. Floyd, J. Ioannidis, V. Paxson, andS. Shenker, "Controlling high bandwidth aggregates in the network,"*ACM SIGCOMM Computer Communication Review*, vol. 32, pp. 62–73, 2002.
[14] R. Mahajan, S. Floyd, and D. Wetherall, "Controlling high-bandwidth flows at the congested router," in *IEEE ICNP*, 2001.
[15] "Worldwide infrastructure security report 2008,"http://asert.arbornetworks.com/2008/11/2008-worldwide-infrastructure-se%curity-report/.
[16]"Cisconetflow,"http://www.cisco.com/web/go/netflow.
[17] Rohit Bhadauria, Sugata Sanyal, "Survey on Security Issues in Cloud Computing and Associated Mitigation Techniques. In *International Journal of Computer Applications* 47(18): pp 47-66, June 2012.
[18] A. M. Lonea, D.E. Popescu, H Tianfield , " Detecting DDoS Attacks in Cloud Computing Environment", *INT J COMPUT COMMUN, ISSN 1841-9836, Feb 2013*
[19] Amazon Web Services: Overview of Security Processes", Whitepaper, March 2013. pp. 1-48. http://awsmedia.s3.amazonaws.com/pdf/AWS_Security_Whitepaper.pdf Science, 1989.
[20]. Ferguson, P. "RFC 2267 - Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing." January,1998.URL:http://www.landfield.com/rfcs/rfc2267.html (27 April 2001)
[21] Carter, Jeff. "Egress Filtering" Version 0.2. 29February2000.URL:http://www.incidents.org/protect/egress.php (27 April 2001)
[22] "5.2.3 Ingress and Egress Filtering" Denial of Service Tools Administration. 5 March 2001.
URL:http://www.tru64unix.compaq.com/faqs/publications/iass/OSIS_53/admin/DNSTLSXX.HTM (27 April 2001)