ISSN:1991-8178

Australian Journal of Basic and Applied Sciences

Journal home page: www.ajbasweb.com

Revealing and Preclusion of DDoS Attack in Cloud Environment

[1]S.P. Chokkalingam and [2]J. Rameshbabu

[1]Associate Professor, Department Of CSE, Saveetha school of Engineering, Saveetha University, Thandalam, Chennai-602105, India.
[2]ME, Department Of CSE, Saveetha school of Engineering, Saveetha University, Thandalam, Chennai-602105, India.

ARTICLE INFO

Article history:
Received 12 March 2015
Accepted 28 April 2015
Available online 1 June 2015

Keywords:
Cloud Computing, Cloud Security, DDoS attack, Intrusion prevention System.

ABSTRACT

The objective of this paper is to detect as well as to prevent DDOS Attack in a cloud environment. The DDoS attack can able to disturb the entire function of cloud server environment. In this paper, we use multiple intrusion prevention system to detect and prevent the DDoS attack. This paper studies all the possible scenarios of DDoS attacks so that the DDoS attack cab be easily detected and prevented in cloud environment. The four possible scenarios of DDoS attack in cloud environments are same requests from a single cloud customer in a same time, more number of different requests from a single cloud customer at a same time, different requests from different cloud users at a same time, requesting a large size file beyond the permitted limit of a cloud user on cloud server. Based on these four scenarios, the DDoS attack is detected and prevented with the help of multiple intrusion prevention system.

© 2015 AENSI Publisher All rights reserved.

To Cite This Article: S.P. Chokkalingam and J. Rameshbabu., Revealing and Preclusion of DDoS Attack in Cloud Environment. ***Aust. J. Basic & Appl. Sci.,*** *9(11): 664-670, 2015*

INTRODUCTION

Cloud computing is the prospect of information technology. It utilizes all the emerging trends in the design and exercise of computer architectures. Also cloud computing technology closely relates other technologies like big data, internet of things. It is an essential transfer to an operational model whereby applications don't live out their lives on. It is the implementation of an improvement and utilization model that replaces hard-wired, proprietary links among software components with light-weight web services and web-based are shared in addition to code. It is the melding of consumer-driven concepts such as self-service with the requirements of enterprise IT. In precise, cloud computing is a junction of technologies and trends that are building IT infrastructures and applications more vibrant, more modular, and more useful. It lets organizations incline up latest services and alter computing resources rapidly, based on business requirements. It gives users self-service access to computing resources, while maintaining appropriate levels of control. And, done right, it provide the means to manage across hybrid computing environments, both on- and off-premise, based on price, capacity necessities, and other factors. The service models in cloud are shown in figure below1.

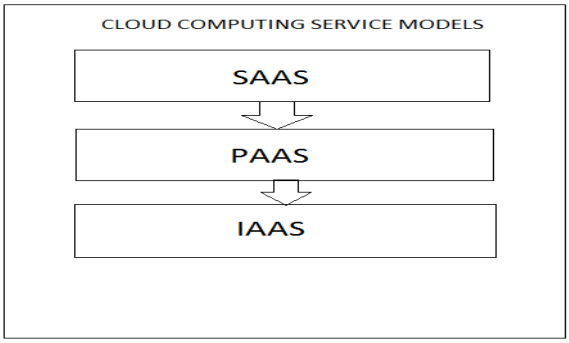

Fig. 1: Service models in Cloud Computing.

Corresponding Author: S.P. Chokkalingam, Associate Professor, Department Of CSE, Saveetha school of Engineering, Saveetha University, Thandalam, Chennai-602105, India.
E-mail: cho_mas@yahoo.com

DDoS attack is considered as a resource management problem. Cloud computing environments always has profound resources, dynamic allocation capabilities. Even though DDoS cannot completely deny the service provides by cloud, it can able to deny the service provided to the individual cloud customers. In this paper, we use the dynamic resource allocation mechanism to tackle DDoS attacks that aim individual cloud customers. In between internet and cloud data center there will be one or more access points which acts as an intermediated between them the intrusion prevention system (IPS) is place on those access point location to monitor and prevent the DDoS attack in cloud. This IPS will monitor all the incoming traffic and able to differentiate between the legitimate traffic from the attack traffic. It will then filters out the attack packets and provides the quality of service (QoS) to the cloud customers. We recommend a dynamic resource allocation mechanism to routinely harmonize the available resources of a cloud to alleviate DDoS attacks on individual cloud customers. The proposed method of dynamic resource allocation technique is easy to implement in any cloud platforms.

DDOS Attack:

The distributed denial of service (DDOS) attack is one of the most commanding attacks used by attackers to damage a company or organization. This attack comes under the category of cyber attacks. The result of this attack causes the services to be temporally unavailable to the legitimate cloud users resulting in a huge potential loss to the individuals and organizations. In recent years, the number of DDoS attack on organization services getting increased. DoS attack is performed by attacker by flooding the attack traffic over the network. This will result in a server crash or server to reboot, making the services unavailable to the cloud customers. The effective intrusion prevention system can be able to counter the DDoS attack. The DDoS attacker first compromise the system to launch a DDoS attack on the victim system. The compromised system will act as a ZOMBIE to perform the DDoS attack on victim system. The architecture of DDoS attack is shown in figure2 below. In figure it is clear that the attacker will compromise many system which acts as a zombie which is under the control of attackers to launch a DDoS attack. All zombie system will then flood the traffic to the victim system to make the victim system to crash and make the services provided by the victim system unavailable to the users of the victim systems.

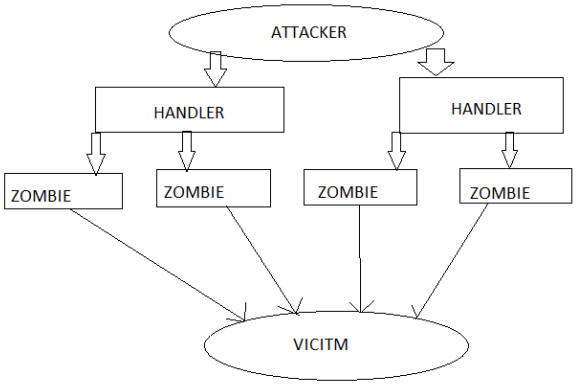

Fig. 2: Demonstration of DDoS attack.

There are many numbers of tools available for launcing the DDOS attacks some of them are listed below.

1. LOIC:

The LOIC stands for Low Orbit Ion Canon which is a simple tool that can be used by single user to perform DDoS attack. It floods an UDP, TCP or HTTP requests to the targeted server.

2. XOIC:

It is another type of DDoS attack tool which is more powerful than LOIC which comes with a GUI to flood the TCP/UDP/HTTP and ICMP messages.

3. HULK:

HULK stands for HTTP Unbearable Load King which can generate a large number of unique requests to flood the traffic. This tool can easily bypass the firewall of the system.

4. RUDY:

RUDY stands for R-U-DEAD-YET tool is a HTTP post DOS attack tool. This tool comes with an interactive user interface. This tool uses an POST method to launch an DDo S attack.

5. Pyloris:

Pyloris is one of the most powerful tools for launching the DDoS attack. This tool uses the SSL and SOCKS proxies to perform a DDoS attack. This tool comes with a simple to use GUI. This tool directly target the service provided by the server.

Australian Journal of Basic and Applied Sciences, 9(11) May 2015, Pages: 664-670

Related Work:

Cloud is one of the leading computing platforms in present scenario. Many individuals and organizations have been placing their critical data's in cloud. So naturally, a question will arise regarding the security of cloud environment. Since the lost of critical data from cloud can cause the huge loss to the cloud users. The DDoS attacks have been place first in the list of security attacks on cloud. The individual cloud hosted servers are considered to be more vulnerable to DDoS attack compared to other cloud hosted servers. In this paper, we are implementing a dynamic resource allocation mechanism to avoid DDoS attacks against an individual cloud hosted servers. Dynamic resource allocation mechanism automatically assign the idle resources of the cloud to clone the intrusion prevention system (IPS) for the targeted servers for quickly filtering the attack packets originates from the botnet master and proving the assurance on quality of service (QoS). DDoS attack can be able to destroy the client server environment but it is not effective against cloud environment. But still it can able to disturb the normal activity of the cloud environment. By using the intrusion prevention system, we can easily filter out the attack packets and guarantee the quality of service to the legitimated cloud customers. In past, single intrusion prevention system is used in the place of access points. But in our proposed system the multiple intrusion preventions systems are used with respect to the victim. The figure 3 and 4 shows the difference in the architecture of existing and proposed system.

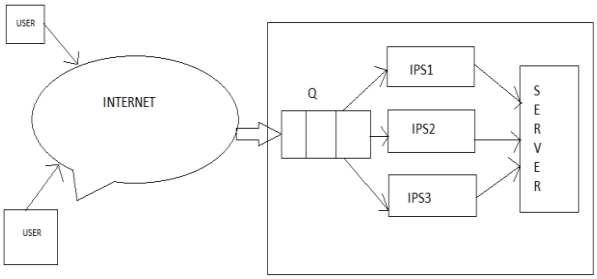

Fig. 3: Architecture of Proposed System.

Proposed Work:

We Deploy Multiple Intrusion Prevention System (IPS) to monitor the Activity of the Users and Filters the Request based on the behavior and forwards to the corresponding Servers through Cloud Server. Each cloud user has certain allocated 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 Behavior Patterns are Continuous and same Request from Single User in a Point of Time, different Query from the Same User within a Period of Time, Different Queries from Different Users but from Same IP, Request of Huge Sized File beyond the Permitted. Based on these Patterns User Behavior is Monitored DDOS Attack is avoided in Cloud. The advantage of proposed system is providing high security by controlling the DDoS attack in cloud environment.

A. Cloud Server Deployment:

Cloud Service Provider (CSP) will normally contains the huge amount of data in their Cloud Storage. The Cloud Service providers also have the overhead of maintaining all the cloud user related information which will be useful for providing the authentication to each and every cloud users. Also the Cloud Server provider will be responsible for passing the requests to the intended cloud server for retrieving the information which is requested by the cloud customer. These Requests are processed by the Resource Assigning Module. The network connection is required between the cloud customers and cloud server to communicate each other. For this Purpose the user interface is necessary for communication between client and cloud server. Assign Module follows the Fist in First out (FIFO) manner for all requests given by the cloud users to cloud servers.

B. Space Allocation:

Cloud Servers is a cloud infrastructure service that allows users to deploy "one to hundreds of cloud servers instantly" and create "advanced, high availability architectures" .The "cloud servers are virtual machines running on the hypervisor for Linux-based instances, and XenServer for Windows and Linux instances. Disk and CPU allocations scale up with memory, with disk sizes ranging from 10 GB to 620 GB. Various distributions of Linux are supported, and each user space allocation with different band width is allocated so they utilizes within the bandwidth.

C. User Mustering:

In this module we tell about the user mustering in that we can able to track Users during an Emergency, ensuring nobody is left in danger zone ,

Reduce Paperwork and Human Error, Data collection and reporting. Get workers back into facility in a safe and timely manner.

D. Deployment Of Multiple IPS:

In this module we implement multiple IPS that is intrusion protection system that used to protect the user form the attacks in existing they were using single to scan the query of a cloud user. But in this proposed module we multiple IPS is deployed to monitor the user query so that it easily find the denial of attack

E. DDoS From Single User:

DDOS is a type of DoS attack where multiple compromised systems which are usually infected with virus, are used to target a single system causing a Denial of Service (DoS) attack. The system which are used to launch a DDoS attack and the attacked systems both are experiencing the DDoS attack. In a DDoS attack, the traffic is flooded to the targeted system from a huge number of sources to launch an attack to make the cloud service unavailable to cloud customers temporally. The difficulty of this attack is to differentiate between the legitimate traffic and attack traffic.

F. DDoS From Multiple User From Same IP:

To launch a DDoS attack, malicious users first build a network of computers that a large number of compromised hosts to probe and check the same addresses in period of time, the spreading rate reduces because the number of the new IP .in this multiple will be login in the same ip address and send query so it will see the account and it will lead to overload on the sever. In out proposed we monitor the query coming from multiple users form the same IP. And we analysis IP address to find the DDOS attack.

G. Attacks Filtering Model:

We present a probabilistic packet filtering (PPF) mechanism to defend the Web server against Distributed Denial-of-Service (DDoS) attacks. In this module the cloud user is blocked if the cloud user requesting a large file beyond its permitted size. Based on these scenarios the DDOS attack is detected and prevented in the cloud environment.

The implementation screenshots are shown in the below figures.

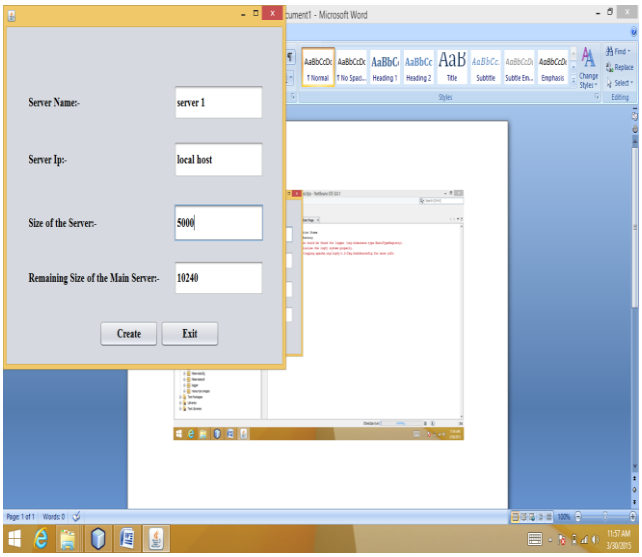

Fig. 5: Creating a Cloud server within the available space.

Conclusion and Future Enhancement:

In this paper, we point out that DDoS attacks are still a successful 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 available resources. Based on this strategy we deploy IPS 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 strategy in a cloud environment. We thoroughly analyze the proposed method. Extensive 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.

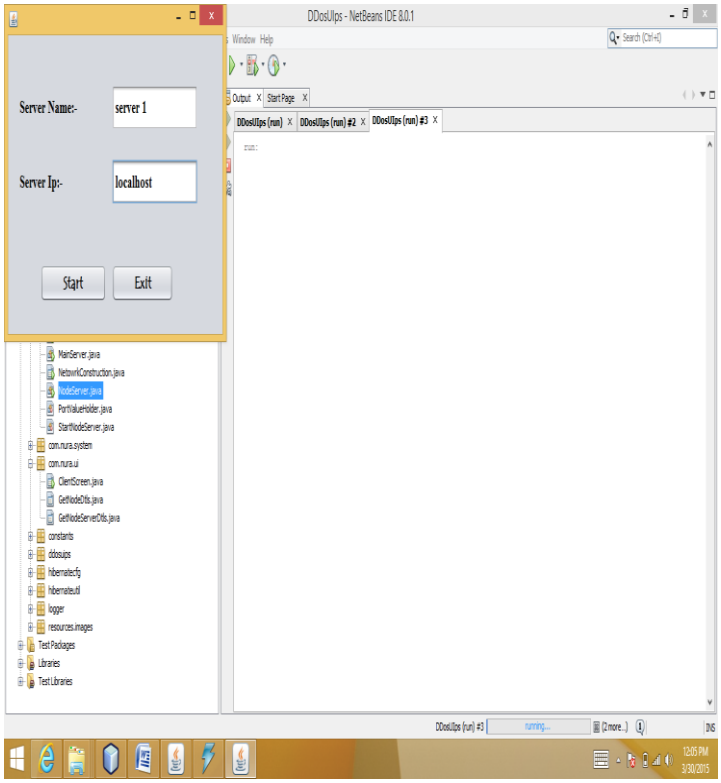

Fig. 6: Cloud Server Initiation.

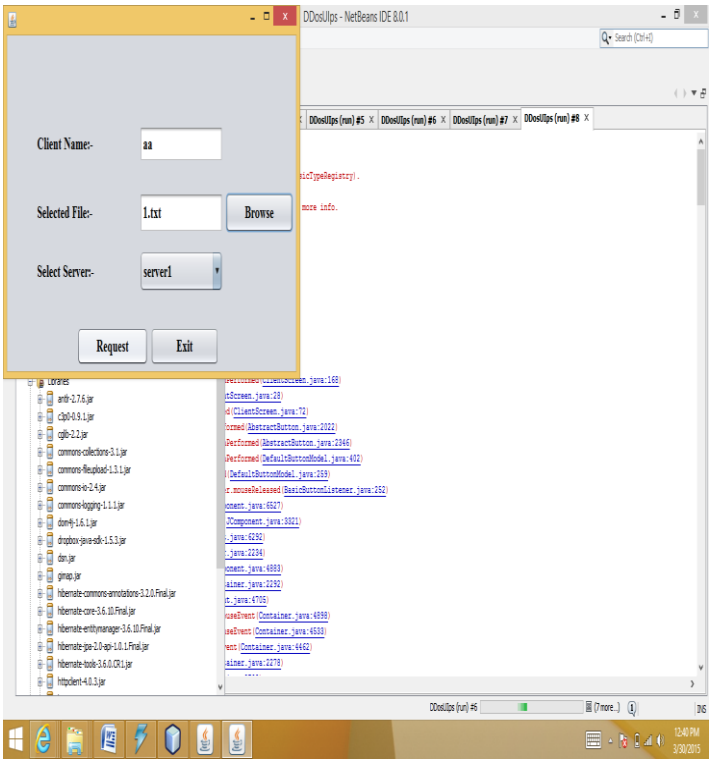

Fig. 7: Client-Side execution.

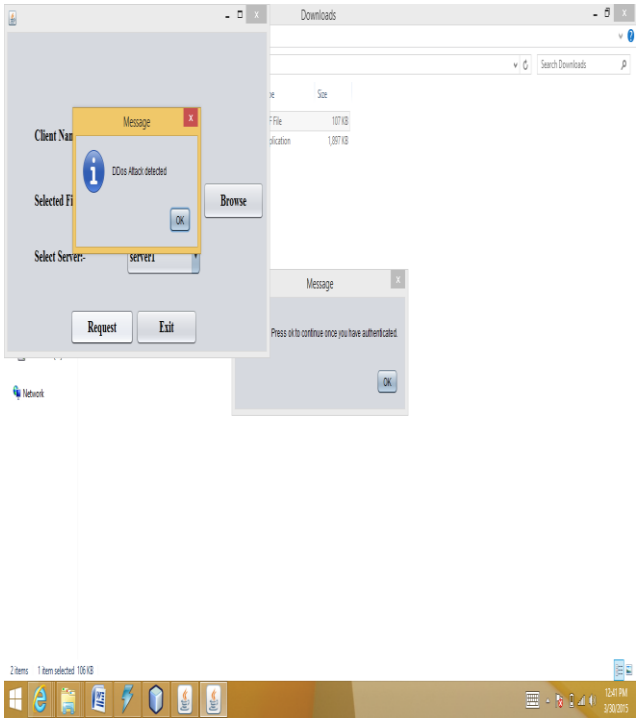

Fig. 8: DDoS attack is detected and warning user.

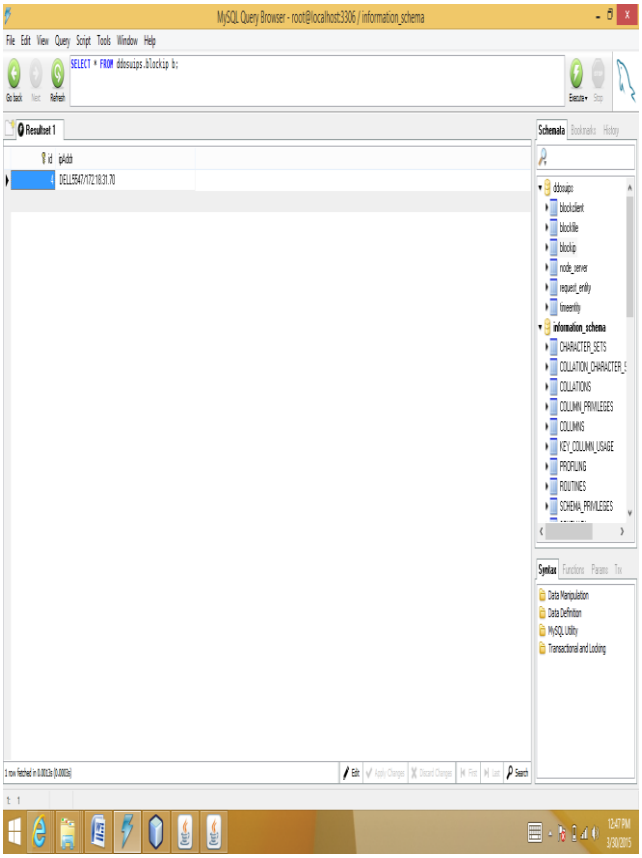

Fig. 9: Attacker IP address information stored in the Database log file.

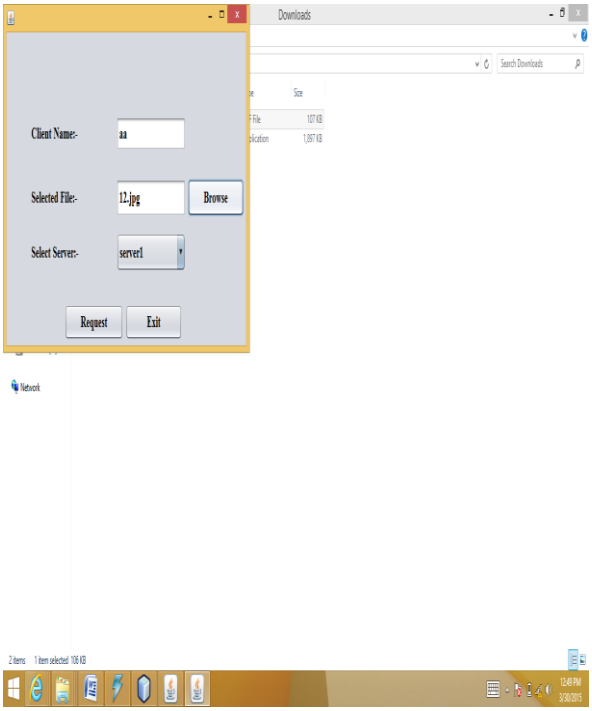

Fig. 10: User attempting to request a large file beyond its limit.

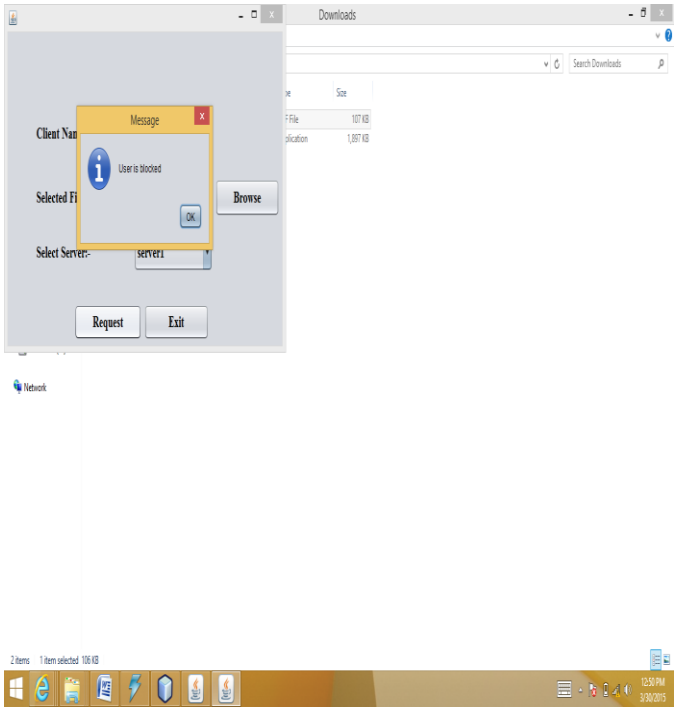

Fig. 11: Repeated DDoS attack is detected and attacker detail stored in database log file.

REFERENCE

Armbrust, M., A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A. Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica and M. Zaharia, 2009. ‘‘Above the clouds: A berkeley view of cloud computing,’’ EECS Dept., Univ.California, Berkeley,CA, USA, Tech. Rep.UCB/EECS-2009-28.

Peng, C., M. Kim, Z. Zhang and H. Lei, 2012. ‘‘Vdn: Virtual Machine Image Distribution Network for Cloud Data Centers,’’ in Proc. INFOCOM, pp: 181-189.

Subashini, S. and V. Kavitha, 2011. ‘‘A Survey on Security Issues in Service Delivery Models of Cloud Computing,’’ J. Netw. Comput. Appl., 34(1): 1-11.

Bhadauria, R., R. Chaki, N. Chaki and S. Sanyal, 2011. ‘‘A Survey on Security Issues in Cloud Computing,’’ CoRR, vol. abs/1109. 5388.

Peng, T., C. Leckie and K. Ramamohanarao, 2007. ‘‘Survey of Network-Based Defense Mechanisms Countering the dos and ddos Problems,’’ ACM Comput. Surv., 39(1): 1-3.

Rajab, M.A., J. Zarfoss, F. Monrose and A. Terzis, 2007. ‘‘My Botnet is Bigger Than Yours (Maybe, Better Than Yours): Why Size Estimates Remain Challenging,’’ in Proc. 1st Conf. HotBots, pp: 5.

Yau, D.K.Y., J.C.S. Lui, F. Liang and Y. Yam, 2005. ‘‘DefendingAgainst Distributed Denial-of-Service Attacks with Max-Min Fair Server- Centric Router Throttles,’’ IEEE/ACM Trans. Netw., 13(1): 29-42.

Yu, S., S. Guo and I. Stojmenovic, 2012. ‘‘Can We Beat Legitimate Cyber Behavior Mimicking Attacks from Botnets?’’ in Proc. INFOCOM, pp: 2851-2855.

Chen, Y., K. Hwang and W.S. Ku, 2007. ‘‘Collaborative Detection of ddos Attacks over Multiple Network Domains,’’ IEEE Trans. Parallel Distrib. Syst., 18(12): 1649-1662.

Francois, J., I. Aib and R. Boutaba, 2012. ‘‘Firecol, a Collaborative Protection Network for the Detection of Flooding ddos Attacks,’’ IEEE/ACM Trans. Netw., 20(6): 1828-1841.

Federal Computer Incident Response Center (FedCIRC), 2000. “Defense Tactics for Distributed Denial of Service Attacks”. *Federal Computer Incident Response Center.* Washington, DC.

www.phreak.org.http://www.phreak.org/archives /exploits/denial/fraggle.c (6 May 2003).

Martin, Michael J., 2002. “Router Expert: Smurf/Fraggle Attack Defense Using SACLS”, *Networking Tips and Newsletters, www.searchnetwork.techtarget.com.* . http://searchnetworking.techtarget.com/tip/1,289483, sid7_gci856112,00.html (6 May 2003).

Chen, Y.W., 2000. “Study on the Prevention of SYN Flooding by Using Traffic Policing”, *Network Operations and Management Symposium, 2000. NOMS 2000. 2000 IEEE/IFIP, pp. 593-604*.

RFC 793, “Transmission Control Protocol DARPA Internet Program Protocol Specification”. Arlington, Virginia. September 1981.

“Nmap Stealth Port Scanner Introduction”, *Insecure.org*. August 2002. http://www.insecure.org/nmap/. (8 April 2003).

“Nessus Documentation”, *Nessus*. 2002. http://www.nessus.org/. (8 April 2003).

“CVE (version 20020625)”, *Common Vulnerabilities and Exposures*. March 27, 2002. http://cve.mitre.org/cve/. (9 April 2003).

“CERT® Incident Note IN-2001-13”. *CERT Coordination Center, Carnegie Mellon Software Engineering Institute.* November 27, 2001. http://www.cert.org/advisories/CA-2001-20.html. (14 March 2003).