Practical Private Cloud Testbed for Studying The Effects of A Botnet Attack

Noor Raad Saadallah Al-Hankawi **Dr. Mohammed Basheer Al-Somaidai**
College of Engineering
University of Mosul
Noor.RaadSaadallah@gmail.com MohammedBasheerAbdullah@gmail.com

Abstract

Many universities and organizations are considering the idea of migrating their data centers to cloud computing. Among the many cloud computing deployment models; the private cloud is the preferred one for such organizations since; it maintains their controllability and enhance security of their servers. Albeit, there are still some risks of attacks. One of these is the Distributed Denial of Service (DDoS) where a large amount of compromised hosts called botnet attacks a specific server causing its service degradation. A test bed for a private cloud computing network was built in the lab making use of Oracle VM Virtual Box as a virtualization environment. This test bed was subjected to a DDoS attack of the SYN-Flood type in multiple scenarios of bots percentage deployment. The same attack was carried out on an Opnet simulation model of the test bed. The results of the practical testbed and the simulation model confirm the devastating effects of such attacks as the botnet size increases.

Keywords: Botnet; DDoS attack; Hypervisor; Private Cloud Computing; SLA; Virtualization.

أنموذج تجريبي عملي لشبكة حوسبة سحابية خصوصية لغرض دراسة هجوم شبكة بوتات عليها

نور رعد سعد الله الحنكاوي **د. محمد بشير عبد الله الصميدعي**
كلية الهندسة
جامعة الموصل

الخلاصة

تعتزم الكثير من الجامعات والمؤسسات تحويل مراكز بياناتها الى الحوسبة السحابية ويعتبر أنموذج الحوسبة السحابية الخصوصية الاكثر تفضيلا في مثل هذه المؤسسات لانه يتيح سيطرة أكبر وامنية أحكم من بقية نماذج الحوسبة السحابية. وعلى الرغم من ذلك لا يخلو هذا الانموذج من بعض الهجمات ومنها هجوم حجب الخدمة الموزع حيث تقوم مجموعة كبيرة من حواسيب المؤسسة المصابة بمهاجمة مخدم معين لغرض خفض أو حجب خدماته عن المؤسسة. بُني في المختبر أنموذج تجريبي عملي لشبكة حوسبة سحابية خصوصية اعتمادا على البيئة الافتراضية التي تقدمها برمجية Oracle Virtual Box وتم تعريض هذا الانموذج العملي لهجوم حجب الخدمة الموزع من نوع SYN-Flood من خلال عدة سيناريوهات يمثل كل منها نسبة معينة من الحواسيب المصابة. تم محاكاة نفس الهجوم على الانموذج العملي من خلال انموذج محاكاة بني باستخدام برنامج Opnet وأُثبت النتائج العملية ونتائج المحاكاة الاثار الكارثية لمثل هذا النوع من الهجمات وخصوصا مع ازدياد نسبة الحواسيب المهاجمة.

Received: 16 – 6 - 2013 **Accepted: 24– 9 - 2013**

1. Introduction

Cloud computing refers to both the applications delivered as services over the Internet and the hardware and systems software in the data centers that provide those services [1]. The applications services are referred to as Software as a Service (SaaS). Some other terms such as Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) are used by vendors to describe the operating systems

software and hardware offered to the clients [2]. When a cloud is made available in a pay-as-you-go manner to the general public, we call it a public cloud, the services being sold are utility computing [3]; where in a service provider manages storage and computing resources on behalf of client over the Internet [4]. The term private cloud (also called internal cloud or cooperative cloud) referred to organizations internal data centers that are available for their members only. Thus only authorized users can access the private cloud services achieving more security and controllability on data and hardware [5]. Private clouds can be deployed in the organization data center or also at a collection facility [6]; making use of the new systems software technique called virtualization; which distinguishes the conventional data center from the cloud based one [7]. In a virtual environment such as the one shown in Fig. (1); the hypervisor plays a vital role in providing each client with different virtual hardware (also called virtual machine) he needs [8].

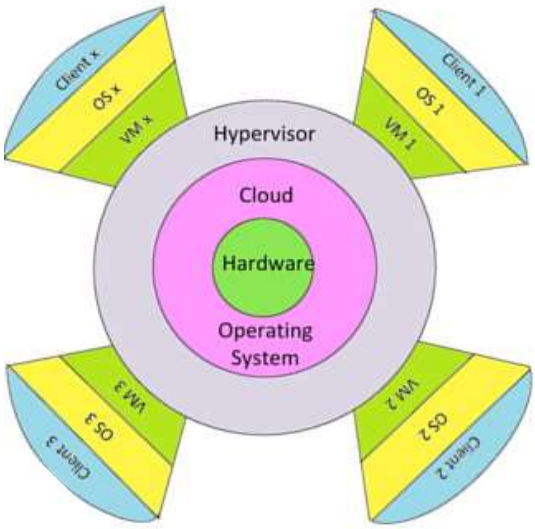

Fig. (1): The role of hypervisor virtualization

Although private clouds are more secure than public clouds due to the limited access list of clients; there are still some vulnerabilities that could be exploited by sabotage attackers to affect the services that are offered. One of these attacks is the Distributed Denial of Service (DDoS) in which the attacker creates an unaware network of compromised hosts to launch a large scale attack upon a specific server that has a specific IP address in order to prevent or degrade services [9]. There are many types of DDoS attacks but the most used one is the SYN-Flood attack in which attackers send a huge number of SYN packets to the victim server causing a lot of corresponding replies and reserving many server resources resulting in its incapability to respond to legitimate traffic [10-11]. In a private cloud computing network the attacker exploits the organization users' computers to participate in the attack without their

desire and knowledge consisting a large network of compromised hosts called bots whish he acts as their master [12]. The SYN-Flood attack and the botnet are illustrated in Fig. (2).

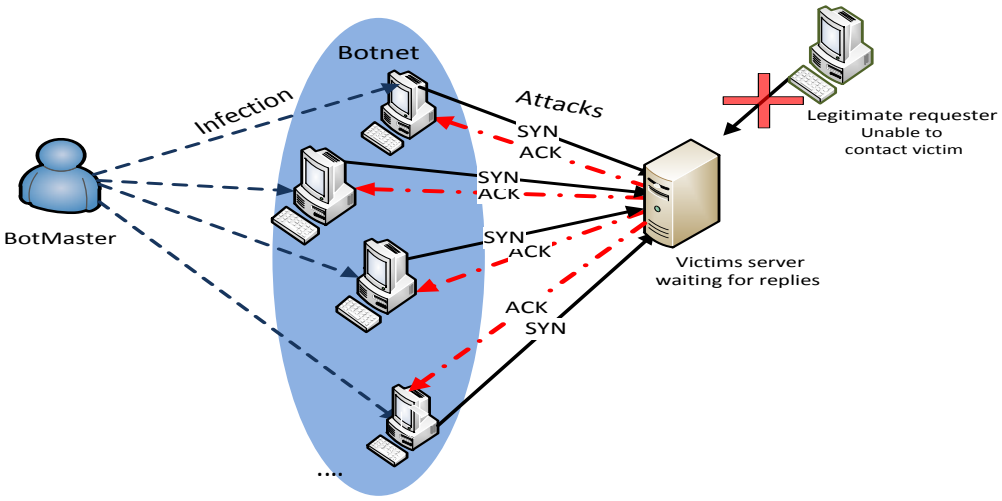

Fig. (2): SYN-Flood attack

2. Related Work

Cloud computing in general and specifically its security issues are rich fields for researchers all over the world. In this section we will give a short review of some papers related to cloud security and DDoS attack. Singh and Jangwal [13] compared between private and public cloud and presented the challenges for building the private cloud and the security issues for it. A quantitative and qualitative comparison among several virtualization environments are presented in [14]. The study concluded that the overall performance of the hypervisor is highly dependent on the algorithms, optimizations, maturity, scalability and the coding strategy used for the hypervisor. The threats and vulnerabilities in cloud computing are summarized in [15]. The paper demonstrated various malicious activities from illegal users that could damage or make an illegal access to critical and confidential data of users or organizations. Ramanaustaite [16] analyzed existing DoS attacks and their counter measures. She simulated two models of these attacks, and then combined them to represent a composite DDoS attack that is more damaging. A simple distance estimation based technique to detect and prevent the cloud from flooding by DDoS attacks is presented in [17]. Han et. at. [18] proposed an automatic and distributed system they called it garlic system to immune the cloud from DDoS attacks. The system is based on the idea of collecting network traffic and then uses the cloud itself to process the huge amount of data collected to discover such attack from the network traffic recorded. Some practical results for the system is also presented.

3. Testbed Model

Our work consists of three parts; the first is building a testbed for a private cloud computing environment that includes five users and a data center. The data center has three servers one for E-mail, the other for HTTP, and the later for FTP services. The second part of the work is applying a SYN-Flood attack to the E-mail server of the data center. The third part is simulating the practical testbed model using Opnet modeler v.14.5 applying the same attack and validating the results and the effects of such attack. The private cloud computing network

consists of five identical hosts characterized as Pentium IV, CPU 3.2GHz, RAM of 2MB and Hard disk of 160GB. All the computers are connected together and to the data center using UTP cables through a 3COM, 24 ports switch. Fig (3) represents the hardware structure of the private cloud computing network testbed architecture. The software architecture shown in Fig (4) consists of four software layers. The upper three layers represent the services that the private cloud offers depending on the services of the virtualization layer. This virtualization layer has been chosen to be (Oracle VM Virtual Box) which supports a variety of user devices and operating systems as shown in Fig (5).

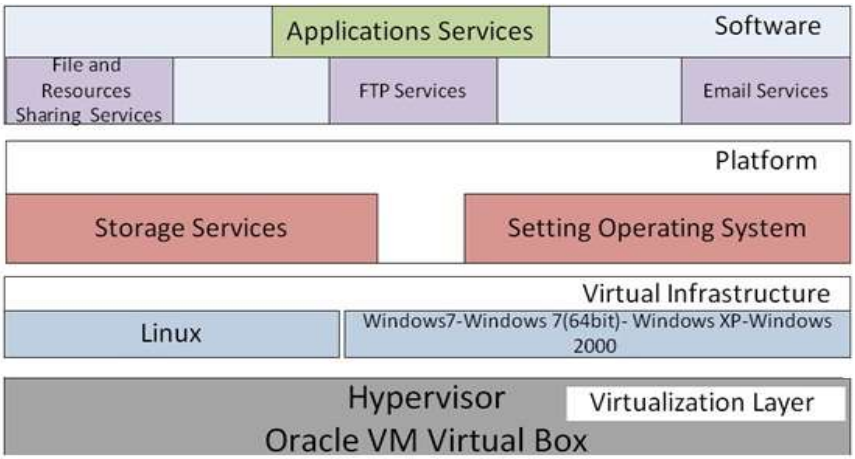

Fig. (4): The Software Layers

Fig. (5): Oracle VM Virtual Box supports many user devices and operating systems

This virtualization layer is installed at the data center regardless of the actual operating system and provides a platform for all the users of the private cloud. Each user creates his account in the private cloud according to a Service Level Agreement (SLA) that organizes his work in the cloud by assigning the virtual hardware and software that he needs. Table (1) illustrates the users' accounts of our private cloud according to SLA.

Table (1): User accounts according to SLA

No. of Client	Operating System	Size of RAM (MB)	Allocated storage space of the hard drive (GB)
1	Windows7 (32bit)	512	20
2	Windows7 (64bit)	512	25
3	Windows XP	192	10
4	Windows2000	168	10
5	Linux	512	8

4. Results and Discussion

The private cloud testbed was operated to maintain the various services provided by the data center and the overall traffic was recorded using Wireshark software. Fig (6) shows such traffic with time, it is obvious that FTP packets were responsible for the majority of the traffic compared to HTTP and SMTP packets which were sent earlier than FTP packets. We imposed this separation of services in time to clearly the traffic amount of the various services never the less, Fig. (7) shows the recorded traffic for the FTP server with various sizes of files being transferred, while Fig. (8) illustrates HTTP packets only.

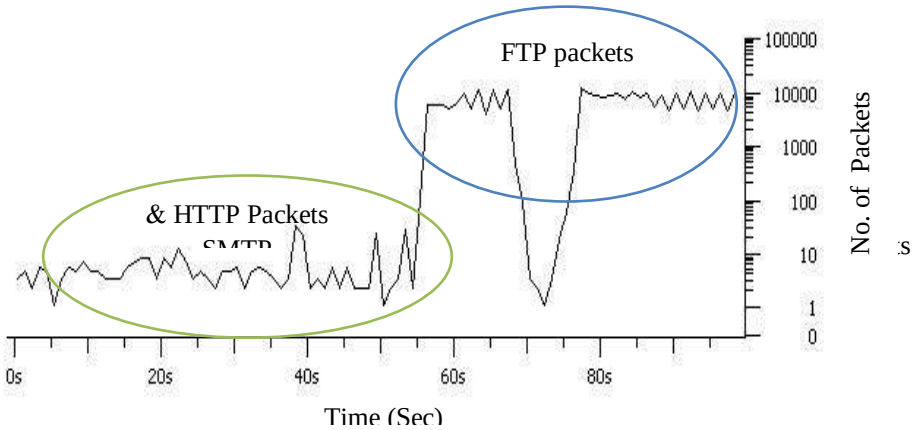

Fig. (6): The number of packets with time for private cloud computing

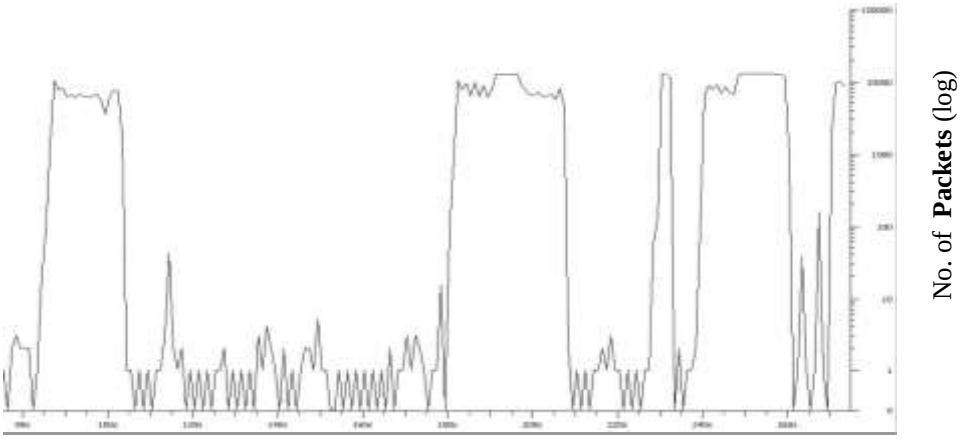

Fig. (7): FTP Packets recorded at the data center

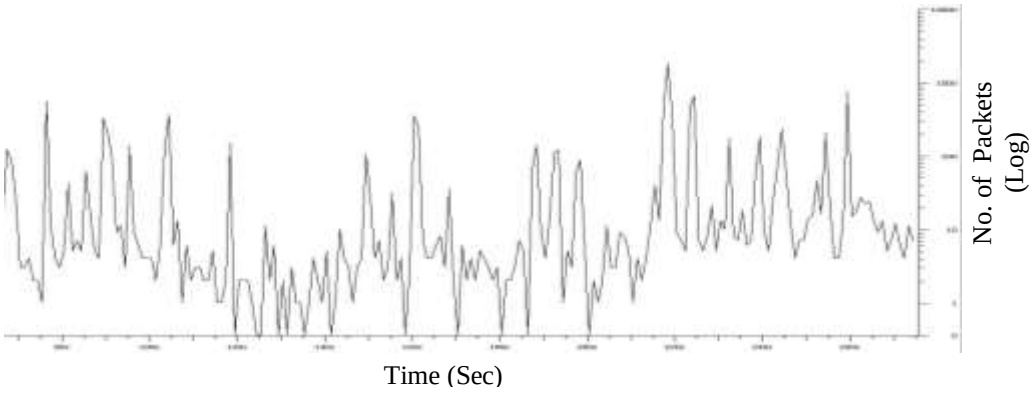

Fig. (8): HTTP Packets recorded at the data center

The E-mail traffic consists of received packets and sent packets providing that all users were on line and sending and receiving E-mails. The recorded traffic at the data center were filtered according to the protocol SMTP and the E-mail server IP address as destination for one time and as a source for the other time, then these statistics were plotted with time in Matlab as shown in Fig. (9).

The spikes in this figure represents attached E-mails with image of (250) KB size. In order to study the effects of botnet attacks upon the E-mail server, several scenarios for the attacks were done. In each scenario the percentage of bots to the total users was increased by 20% thus, six scenarios were conducted for the DDoS attack referring to (0%, 20%, 40%, 60%, 80%, and 100%) of bots. The attack was conducted using Engage Security Ver. 2.2.0 of the type SYN-Flood at 1800sec of the recorded time of one hour operation.

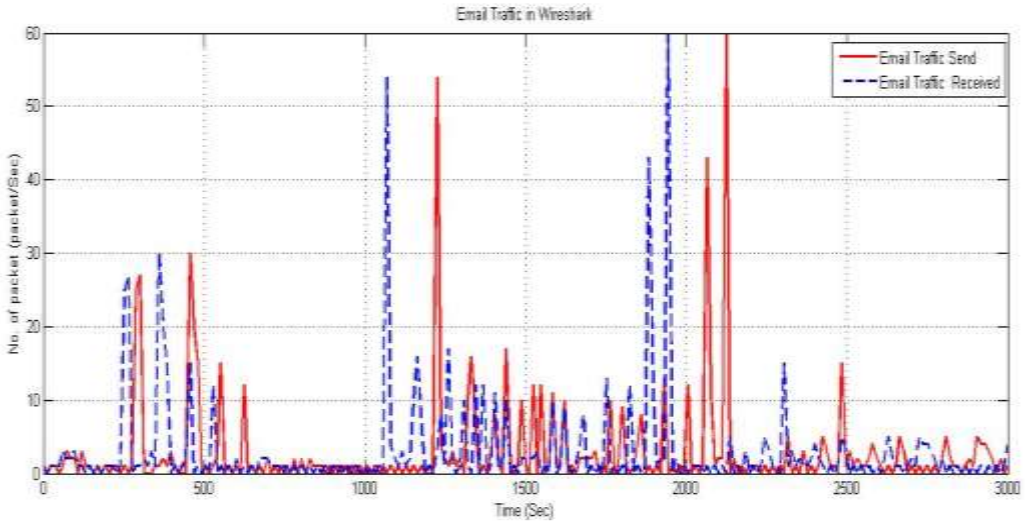

Fig (9): Received and Sent E-mail packets in the data center

The recorded Wireshark traffic were exported to Matlab and averaged for every 150 seconds after the first 150 Sec which was excluded from the results this period was reserved for initiating the connection. The Matlab results are illustrated in Fig. (10). It is obvious that the number of packets is proportional to the bot percentage in the private cloud after attack. The simulation model for the practical testbed was carried out using Opnet Modeler with the

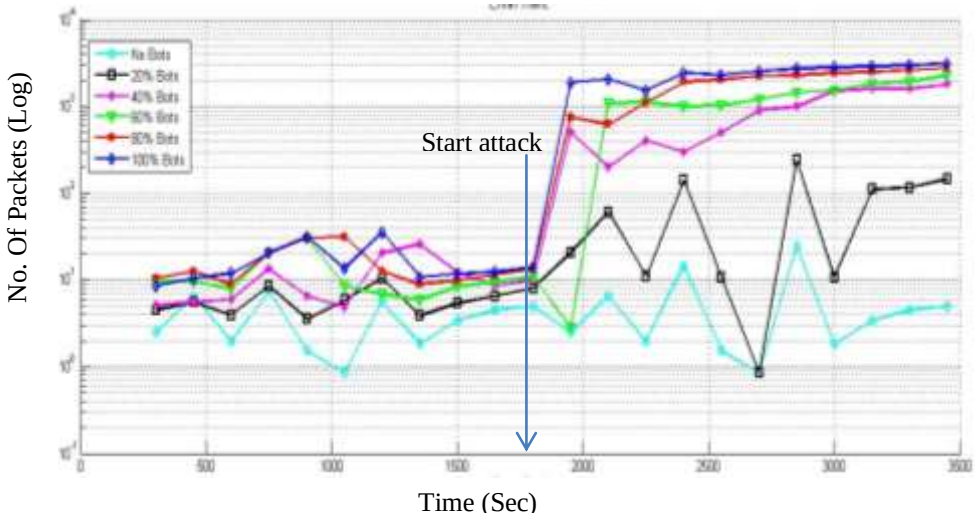

Fig. (10): E-mail traffic received after DDoS attack

same parameters as shown in Fig. (11). Two global statistics were chosen. The first is the E-mail received packets in (packets/Sec) which counts the arrived rate of E-mail valid application packets in the whole network. This is calculated on the basis of statistical data coming to the application from the transport layer, therefore SYN-Flood attack this statistic is illustrated in Fig. (12). The second global statistic is the Ethernet delay in (Sec) which measures the layer two delay for all the network frames including SYN-Flood attack frames. Table (2) demonstrates the average values of the above two global statistics for multiple bot percentage deployment scenarios.

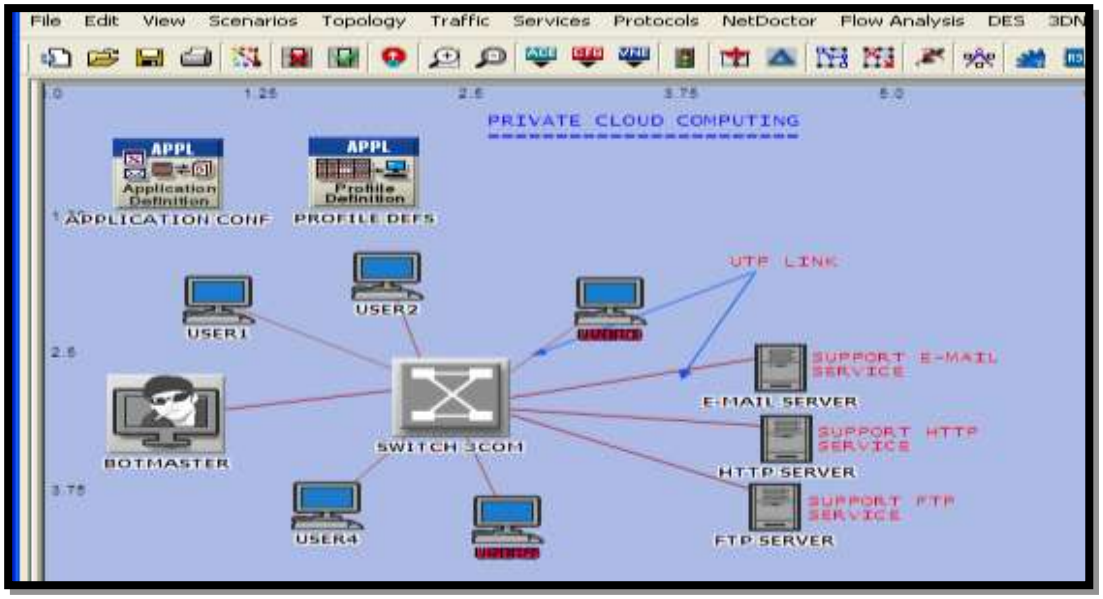

Fig. (11): Network model of the private cloud computing

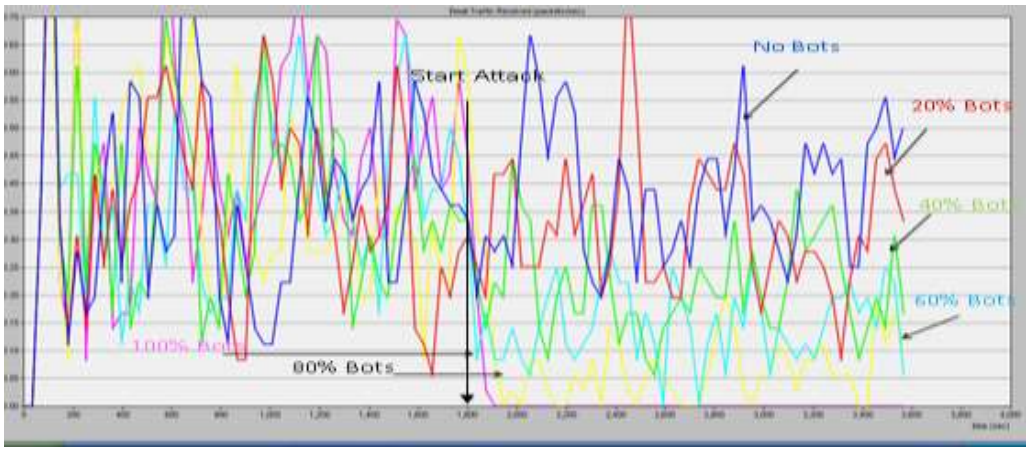

Fig. (12): E-mail traffic received (packet/sec)

Table (2): Global statistics registered in Opnet program after applying DDoS attack

% of Bot Deployment	Average E-mail Received Traffic (Packet/Sec)	Delay (Sec)
0%	0.3647	13.2
20%	0.3479	13.5
40%	0.3469	13.6
60%	0.3042	13.856
80%	0.2264	14.54
100%	0.1967	14.558

It is clear from the table that increasing bot percentage deployment decreased legitimate E-mail received packets and increased Ethernet delay. The attack time is a crucial factor for this table data since it averages the whole statistic along the simulation time (i.e. before and after the attack) and this attack time is chosen to be at 1800 Sec of the one hour simulation time for similarity with the practical test bed. In order to display the botnet attack effect on the E-mail server; Table (3) presents the percentage E-mail service degradation after the attack. Comparing the results of practical testbed with the simulation model is important to validate both models

Table (3): The percentage decrease in E-mail received packets increase the bots deployment in the network

%of Bot Deployment	Average E-mail legitimate packets after attack(packets)	% of service degradation
0%	0.404	%0
20%	0.355	%12
40%	0.279	%30
60%	0.166	%60
80%	0.066	%83
100%	0.000	%100

Figure (13) illustrates the normalized no. of IP packets recorded for the 100% bot scenario for both models. It is clear that there are very matching trend for the two models especially after the attack.

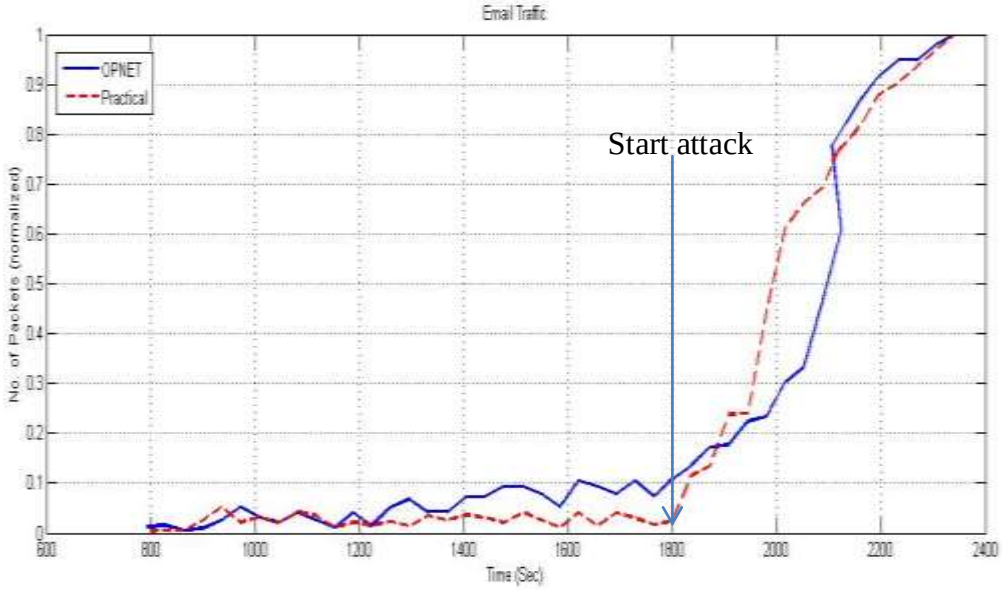

Fig. (13): Comparison of the results of the testbed model and simulation model for 100% bots

5. Conclusions and Future Work

Private cloud computing network is a good choice for big organizations that want to benefit from the new cloud paradigm and in the same time maintain security and controllability upon their servers and critical data. Never the less, there still many vulnerabilities and security issues that these organization should worried about one of these is the Distributed Denial of Service (botnet) attack. In this paper we tried to implement such attack on a private cloud network testbed and study its effects on the services that it offers. A simulation model is also conducted validating the practical results. The main criterion of this paper was the percentage of bot deployment in the network. The results showed the crucial effects of this attack on the network especially for large bot percentage deployment. Therefore, more studies should be made to predict and countermeasure such attacks.

References

[1] Waschke, M., "Cloud Standards Agreements That Hold Together Cloud", CA Press, Distributed by Springer and Bussiness Media, NewYork, 2012, pp. 1-23.

[2] Reddy, V.K., and Reddy, S.S., "Security Architecture of Cloud Computing", International Journal of Engineering Science and Technology (IJEST), Vol. 3, No. 9, September 2011, pp. 7149-7155.

[3] Winkler, J.R., "Securing The Cloud: Cloud Computer Techiques and Tactics", Elsevier Inc.,/ MA/ USA, 2011, p. 33.

[4] Horwitz, L., "Building a Private Cloud", E-publications, Data Center and Virtualization Media Group, TechTarget Inc., 2013, pp. 1-17.

[5] Horwitz, L., Kleyman, B., and Jennings, R., "Private Cloud Strategies for Building a Private Cloud", TechTarget Inc., Vol. 2 , No. 1, February 2012, pp. 2-14.

[6] Smoot, S. R., and Tan, N. K., "Private Cloud Computing, Considration, Virtualization, and Service-Oriented Infrastructure", Elsevier, Inc., USA, 2012, pp. 45-153.

[7] Shackledford, D., "Virtualization Security Protecting Virtualized Environments", John Wiley and Sons, Inc., /Indianapolis/ Indiana/ Published Simultaneously in Canada, 2013.

[8] Schulz, G.,"Cloud and Virtual Data Storage Network", Taylor and Francis Group, LLC, U.S., 2012, p. 16.

[9] Sperotto,A., and Pras, A., "The Effects of DDoS Attacks on Flow Monitoring Applications", IEEE, 2012, pp. 269-277.

[10] plohmann, D., Padilla, E.G., and Leder, F., "Botnets: Detection, Measurement, Disinfection and Defence", European Network and Information Security Agency (ENISA), 2011, pp.1-153.

[11] Upadhyaya, A., Jayaswal, D., and Yadav, S., "Botnet: A New Network Terminology", Emerging Trends in Networks and Computer Communications (ETNCC) International Conference, IEEE, 2011, pp. 424-428.

[12] Liu, Ch., Lu, W., Zhang, Z., Liao, P. and Cui, X., "A Recoverable Hybrid C & C Botnet", 6th International Conference on Malicious and Unwanted Software, IEEE, 2011, pp. 110-118.

[13] Singh,S. and Jangwal,T., "Cost breakdown of Public Cloud Computing and Private Cloud Computing and Security Issues", International Journal of Computer Science and Information Technology (IJCSIT), Vol. 4, No. 2, April 2012, pp. 18-30.

[14] Sridharan, S., "A Performance Comparison of Hypervisors for Cloud Computing", Msc. Thesies, University of North Florida School of Computing, Florida , August 2012, p. 112.

[15] Bamiah, M.A., and Brohi, S.N., "Seven Deadly Threats and Vulnerabilities in Cloud Computing", International Journal of Advanced Engineering Sciences and Technologies (IJAEST), Vol. 9, Issue. 1, 2011, pp. 87-90.

[16] Ramanauskaite, S., "Modeling and Research of Distributed Denial of Service Attacks", Ph.D Thesies, Vilnus Gediminas Technical University, VGTU Leidykla Vilnius Technika, 2012, p. 107.

[17] Katkamwar, N.S., Puranik, A.G., and Deshpande, P., "Securing Cloud Servers against Flooding Based DDoS Attacks", International Journal of Application or Innovation in Engineering and Management (IJAIEM), Vol. 1, Issue 3, November 2012, pp. 50-55.

[18] Han,F., Chen, Z., Xu, H.F., and Liang, Y., "Garlic: A Distributed Botnets Suppression System", 32nd International Conference on Distributed Computing Systems Workshops, IEEE Explore, 2012, pp. 634-639.

The work was carried out at the college of Engineering. University of Mosul