Simulating the Resource Freeing Attack: Using Cloudsim Simulator

Shakiba Nayebalsadr

MSc. Studetnt, School of Computer Engineering, Iran University of Science and Technology, Tehran, Iran
Sh.nsadr@cmps2.iust.ac.ir

Morteza AnaLoui

Associate Professor,School of Computer Engineering, Iran University of Science and Technology, Tehran, Iran
analoui@iust.ac.ir

Abstract—Virtualization technology is recognized as an infrastructure for cloud computing. Actually, the virtualization is a technique which is able to make the cloud computations secure. However, virtualized environment could be vulnerable to some security issues such as lack of performance isolation. These days, using the virtualization as a technique which is able to reduce the costs and increase the reliability of the systems by means of sharing the physical resources between several virtual machines, has grown saliently in large organizations. Despite of these advantages, virtualizations have made several security challenges too. So, the main concern of virtualization services providers and their costumers is how to detect and encounter these security challenges. In this research the resource freeing attack is selected among all available virtualization's attacks because of its simplicity in performing and its drastic effects. After simulating the attack, the CPU's efficiency, response time diagrams, and the obtained bandwidth are measured. The simulation results show the significant changes in virtual machine behavior. These changes help cloud provider to detect resource freeing attack in the cloud.

Keywords—Security, Virtualization, Cloudlet, Resource Freeing attack , Cloudsim.

I. I .INTRODUCTION

The virtualization and security are among the most important issues in cloud computation. Thus, paying attention to the virtualization threats and attacks is necessary. The virtualization techniques make several virtual machines able to use the physical resources of the system commonly [1]. This technology introduced by IBM in the late sixties. In spite of several offered advantage for the users there are several security challenges for the virtual machines using this technology [2]. Most of the security challenges existing in virtual machines are similar to physical machines. However, there are some security challenges and attacks which are appertained to the virtualization. One of these challenges is the resource freeing attack which is discussed in this research. This challenge has no solution because of following reasons:

-It has risen recently.

-It is using the natural behavior of the virtualization.

In this research, we have reported a summary of the related works to our subject in the first section. In the second section, we have introduced the resource freeing attack, the conceptual design of the attack and the performance of the attack. In third section, we have simulated the attack using cloudsim simulator and the results were obtained in forth section and in the last section we using the averaged values between 30 simulations, the corresponding diagrams have been plotted and after that, the CPU utilization diagrams in addition to the bandwidth diagrams before and after the attack are plotted and the variation of the bandwidth output versus time is discussed.

II. RELATED WORKS

Studying the history of the attack simulation using cloudsim makes it clear that the only attack which is done in the cloud environment using cloudsim is the DDOS attack. These days, there are some defensive mechanisms in order to diagnose and reduce the DDOS attack threats in cloud computations. For example, Palvinder et al. developed an algorithm based on analytical procedure in order to reduce the DDOS attacks over cloud. Their results make it clear that performing the simulations using cloudsim tool could be an effective action in order to oppose the DDOS attack [3].

DDOS attacks over the World Wide Web are become to a considerable issue for the computer researchers in Iran University of science and technology. DDOS attacks don't excite easily and their identification and opposition is a challenging task. These features have made this attack to an interesting tool for hackers. Since the DDOS attacks don't have a familiar formation, so the existing methods couldn't identify them completely and it needs high skills. Regarding to the performed researches, the only simulated attack using cloudsim simulator is the DDOS attack and there isn't any suggested procedure for performing the resource freeing attack using this simulator up to now. So, we would simulate the

resource freeing attack using cloudsim simulator in this research.

Generally, having two running cloudlets, while having no interference between their performances, would make the resource freeing attack happen. Side-channel attack is among the resource freeing attacks.

In a side-channel attack, the attacker gains information about the cryptographic technique used by analyzing physical characteristics of the cryptosystem implementation. The attacker uses information about the timing, power consumption, electromagnetic leaks and etc. to exploit the system. This collected information can be employed in finding sensitive information about the cryptographic system in use. In cloud computing, side-channels attacks are conducted through gaining access to the physical node hosting the target VM.

Resource-freeing attacks (RFAs) are a new type of attack in the Cloud that exploit the co-residency and resource sharing among VMs in order to modify the workload of a victim VM to release resources for an attacker VM Any hypervisor such as Xen tries to provide performance isolation by allocating required resources to each VM.

A hypervisor scheduler may provide a fair-share allocation of the processor by distributing idle processor time to running VMs (work-conserving), or by putting a limit on the maximum amount allowed for each VM (non-work-conserving). The former increases performance, but reduces isolation, whereas the latter increases the isolation with the cost of decreasing the performance. A resource-freeing attack occurs when a work-conserving scheduler is used. The first step to launch an RFA attack is to increase the resource usage of the victim so that it reaches a bottleneck.

This step is performed by using a helper process that can be run either on the same or another machine. Then, the next step would involve shifting the victim's resource usage to the bottleneck resource. This would free up other resources to be used by the attacker [4].

A. The Security of the virtualization

Nowadays the virtualization is known as a basic technology in the cloud computation structure and has made it possible to run the software independent of the hardware in cloud environment. Furthermore, making a high flexibility it is possible to assign resources such as percentage of the active processor or active memory to the computations with respect to the user demand. So, making the virtualization secure would assure the data and service's security. These days, using the virtualization as a technique which is able to reduce the costs and increase the reliability of the systems by means of sharing the physical resources between several virtual machines has grown saliently in large organizations. Despite of these advantages, virtualizations have made several security challenges too. So, the main concern of virtualization services providers and their costumers is how to detect and encounter these security challenges [5,6]. In this research the resource freeing attack is selected among all available virtualization's bed attacks because of its simplicity in performing and its drastic effects and would be simulated using cloudsim simulator.

B. Threats and vulnerabilities in the virtual environment

The virtualization had been faced with security threats as an important technology before cloud computations and has transferred these threats to the cloud environment itself. In hypervisors all users know their own systems as isolated ones even if they are feeding by the same machine. In this structure a virtual machine is an operating system which is controlled via a control program through a sub-layer [5] . The existing threats in the virtualization environment could be listed as bellow [7].

1. Observing the virtual machine through the host machine

2. Observing the virtual machine through a different virtual machine

3. Back doors in virtual machine

III. INTRODUCING CLOUDSIM SIMULATOR AS THE ATTACK SIMULATOR TOOL

Cloudsim is a simulation tool which could perform the modeling, the simulation, testing the cloud computing sub-layers and services for the new users. Cloudsim tool models the behavior of system components such as data centers, virtual machines and resources preparation policies and would build some common techniques in order to limit the tasks and make them simple. Actually, cloudsim tool supports modeling and simulating the cloud computational environment in isolated clouds or inside the network. The cloud federation and cloud users interfaces make some policies in order to assign the virtual machines in cloud computational scenarios inside the network. Many researchers in HP institutions in USA use cloudsim tool as a cloud resources provider and an effective energy controller [8,9]. There are a lot of classes in cloudsim environment which are used in network, power, scheduling and etc. regarding the demands of the user. A series of important classes which are used in simulating the attack are scheduling timeshared and scheduling space shared classes which are discussed in next section.

A. Definition of spaceshared and timeshared scheduling in cloudsim

When we have several cloudlets on a virtual machine, the challenge is to classify the CPU and bandwidth. Performing the classification could be done as following:

1.Space-shared scheduling: It means that the CPU and bandwidth are shared between all virtual machines equally.

2.Time-shared scheduling: The total capacity of the CPU and bandwidth is assigned to a cloudlet in a specified time interval and after that in the next time interval all these capacities are assigned to another cloudlet.

Cloudsim tool provides the virtual machines in 2 classes which the first one is in the host level and the second one is in the virtual machine level. For simulating the attack, we have applied the space-shared scheduling in the virtual machine level [7].

IV. RESOURCE FREEING ATTACK

The resource sharing nature in virtualization would cause a unique attack which is named as resource freeing attack. This attack reports at 2012 for the first time and is related to the 2 different virtual machines over a same physical machine. The basic idea of this attack is the virtual machine which needs to the resources more than the shared portion, would change the loading of one or more other virtual machines over the same physical machine and would convince the hypervisor to assign more portion of resources to the attacker [10].

One of the main tasks of the hypervisors is the performance isolation. Performance isolation means the performance of a virtual machine doesn't affect another virtual machine's performance. However, the experiments show that the Xen hypervisor wouldn't perform the performance isolation effectively.

A. Conceptual scheme of the attack

The attacker consists of two parts: beneficiary and helper. The beneficiary is the process or parameter which the attacker wants to improve it. The helper is the process or program which helps the attacker to change the loading of the victim. This program could either be in the attacker machine or in another physical machine. Furthermore, it is assumed that the utilization level of the beneficiary doesn't reach to a desired level [11].

In this attack the beneficiary and the attacker would help each other in order to change the loading of the victim in a way that the utilization of another unwanted resource is increased in the victim machine and utilization of the target resource is decreased. This way, two main necessities are considered as following:

1.The attacker needs to increase the consumption of a resource in the victim machine to the extent that becomes as the crisis of the victim's machine. This way it is impossible for the victim machine to utilize any other resources such as target resources.

2.The attacker needs to change the utilization time of other resources in the victim machine in order to make the victim to assign less time to the target resource and this way the target resource would be released.

Generally, the attacker could change the portion of the victim two ways:

1.Forcing the victim to utilize the target resource less

2.Changing the victim's utilization time of a resource (without changing the victim's portion of the target resource)

B. performing the attack

The attacker could change the victim resource consumption pattern in two ways:

1.changing the victim resource consumption pattern inside the victim machine

2.changing the victim resource consumption pattern outside the victim machine

3.Changing the victim resource consumption pattern could be done by means of the beneficiary or by helping the outside helper which is responsible to change the victim's resource consumption pattern only and doesn't benefits of the attack.

V. SIMULATING THE ATTACK USING CLOUDSIM SIMULATOR

For simulating the attack in cloudsim simulator tool, we have first defined the simulation time which is equal to 24 hours in the present study. Since we are simulating the attack using simulator tool, the real elapsed time is about a few seconds.

In this section the CPU utilization is measured. Therefore a datacenter is created in cloudsim including a host which contains two different virtual machines. The properties of these objects are defined as following. The measurements are performed over the first machine at first and after that the second machine is added.

The properties of objects which are defined in the laboratory:

A. Object properties:

The host properties:

Arch = "x64";

OS = Linux;

VMM = "Xen";

RAM = 64GB;

Host with 12 core and each core 2400 MIPS;

The virtual machine properties:

RAM = 2GB;

1 core of CPU;

The transferred requests to the virtual machine are in the of CPU consuming objects which are named as cloudlets:

Length = 50000MI;

Utilization Model of CPU and BW and RAM = Full;

These requests are sent to the virtual machine with exponential distribution with the rate of 100 requests per seconds

VI. Results & Implementation

Diagrams obtained at the end of CPU measurements in different states are as follows. The applied data values in diagrams are based on averaging of 30 simulation measurements. The reason of averaging is the randomness nature of generated values. Generally, the values of utilization don't have any effect on physical elapsed time. We have measured the values of the utilization in intervals equal to 5 minutes (300 seconds). In the following diagrams the performance of the processor is plotted by means of both the λ performance and the average inverse formulations through collecting the output data.

$$R=CPU\_UtilizationLambda/1-CPU\_Utilization \quad (1)$$

In this Formula ‹R is the response time per second and CPU_Utilization is the Efficiency of the processor versus bandwidth in percent and lambda is the rate of requests

$$CPU\_Utilization=S*Lambda \quad (2)$$

in the equation above, S is the total response time to the requests. Using the obtained results from the simulation, we can plot different values of the parameters. Following are the diagrams obtained from averaging between the results of 30 simulations performed in the first part of the research.

Figure 1 shows the CPU performance (measured) versus different λs. In this figure the measurement process is based on the portion of the service time to the total time. The x axis is representative of λ variations and the y axis is the average performance.

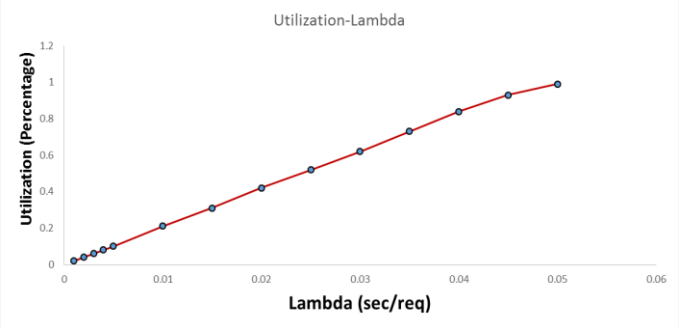


Fig. 1. The diagram of CPU performance (measured) versus λ

During the simulation, the time step between 2 requests for the total requests is measured and averaged. So the following diagram is the performance changes versus inverse of the average. The measurement procedure of the performance in this diagram is to multiply the time service to the inverse of the average. The x axis is the representative of 1/mean and y axis is representative of averaged performance.

Figure 2 shows the response time (measured) versus CPU performance (measured).

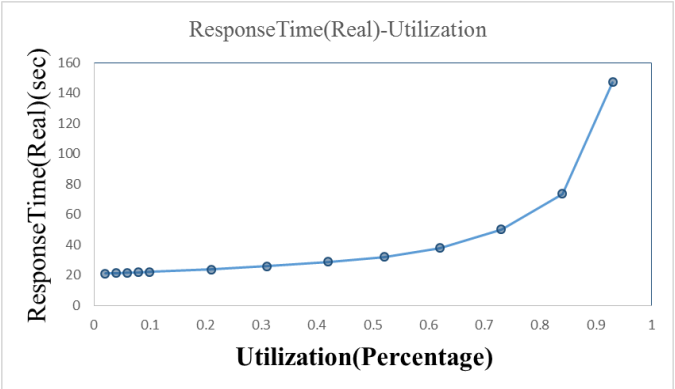


Fig. 2. The diagram of response time (measured) versus CPU performance (measured).

Following are the measurement of CPU utilization and bandwidth in 5-minutes periods. This way, the intervals related to the attack could be diagnosed more precisely. These diagrams are covering both the after and before attack states and would be discussed in following. .

A. diagrams of bw and cpu variations before and after the attack

In this section using the exponential distribution and the rate of 1/λ, random numbers are generated. The created exponential number is the distance between two submission times which is the time for sending the cloudlets to the virtual machine. In the other words, we would have a time step based on exponential distribution which the corresponding created cloudlets are based on the exponential distribution.

The main objective of this article is to prevent the CPU from bottlenecking with respect to the behavior of the cloudlets. It is worth to say that in this research we have to pay attention to the corresponding cloudlet of each attack. Furthermore, we have to say that the present research is discussed the virtual machines and cloudlets which are assigned to the virtual machines. Actually, during running the cloudlets each one occupies a portion of the CPU and when the process in finished next cloudlet runs. In other words, cloudlets share CPU with each other. In this research, we have used the spaceshared method. This way each cloudlet occupies the whole CPU each time and after finishing the process next cloudlet occupies the whole CPU immediately. This way, some cloudlet may either be in queue and waits for the processing time or be in the system and runs to the process immediately after freeing the CPU. Actually we can say the service time would be equal to the simulation start time if the waiting time is zero. It means that:

$$WaitingTime + SubmitionTime = Start\ \ Time \quad (3)$$

Regarding to the provided explanations we would discuss the diagrams of the variations of output (delta throughput) versus time for each bandwidth and the processor utilization versus time before and after the resource freeing attack and would compare these two states.

In this research we used Microsoft excel in order to plot the diagrams at first. An example of these diagrams is depicted in Figure 3 as the variations of output bandwidth before and after the attack.

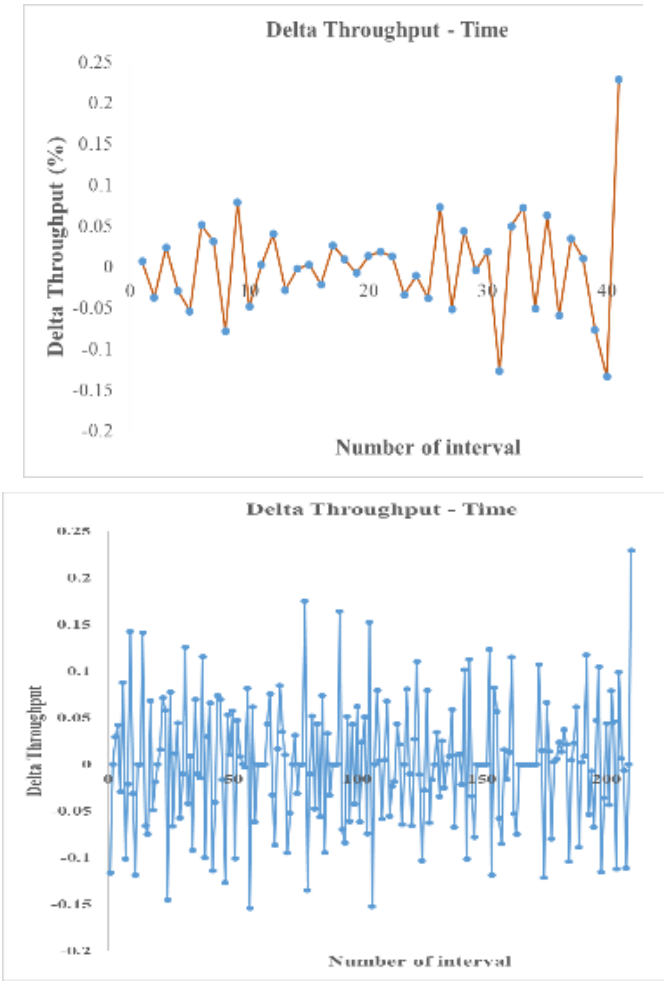


Fig. 3. Variations of output bandwidth before (up) and after (down) the attack

As it is shown in figure 3, there are a lot of time varying details which could not be easily extracted from this type of diagrams. So, we have used another type of diagrams which are named as Fast Fourier Transform (FFT) which could relate the time varying phenomenon as a function of frequency of the changes and each frequency corresponding power density. When trying to interpret time-sequence data from a transient solution, it is often useful to look at the data's spectral (frequency) attributes. To interpret some of time dependent data, we need to perform Fourier transform analysis. In essence, the Fourier transform enables us to take any time dependent data and resolve it into an equivalent summation of sine and cosine waves. We have used the fluent software in order to plot FFT diagrams. The x axis of the diagrams is the representative of the frequency (Hz) and the y axis is the representative of signal value squared (Power Spectral Density).

B. Comparing the bandwith output variations versus time

In this research the bandwidth throughput and CPU utilization diagrams are plotted using FFT technique. Figure 4 represents the diagram of the bandwidth output variations versus time before and after the attack. The main points in these diagrams are the sharply breaking ones which are indicative of the overload and shortage of the load over the victim machine.

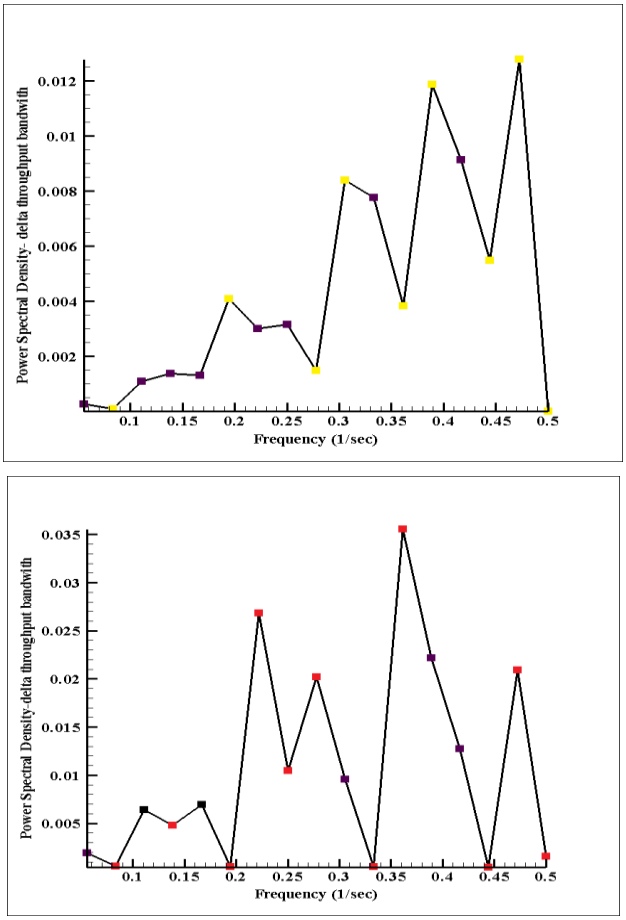


Fig. 4. The diagram of the bandwidth output variations versus time before (up) and after (down) the attack

The attack scenario is the way that when all cloudlets are using the same percentage of the CPU and bandwidth, a unique cloudlet either occupies other cloudlets portion of the CPU or the bandwidth and the victim cloudlets would be engaged with the remained portion of CPU or bandwidth.

Regarding to the figure 4 the frequencies equal to 0.194, 0.306, 0.389 & 0.472 Hz are representatives of the overload situations before the attack. In the other words, cloudlets have the maximum value of the bandwidth at these frequencies and either have normal or shortage of the load at other points. After performing the attack, the cloudlet's bandwidth reaches its maximum loading at frequencies equal to 0.139, 0.222, 0.278, 0.361 & 0.472 Hz. According to the critical frequencies, it is seen that the frequency equal to 0.472 Hz is common before and after the attack. So, we could say this

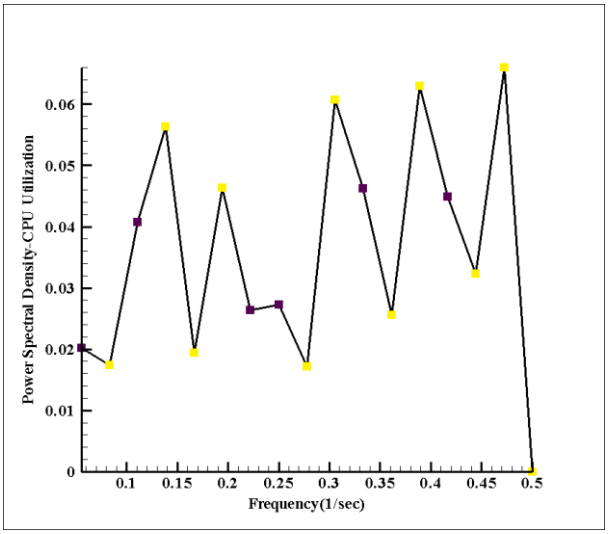
frequency is not affected by the attack. This way, it is concluded that the attack has destroyed the frequencies equal to 0.194, 0.389 & 0.306 hertz and has created the new ones equal to 0.139, 0.222, 0.278 & 0.361 hertz.

Furthermore, regarding to the figure 4 the frequencies equal to 0.0883, 0.278, 0.361, 0.444 & 0.5 Hz are representatives of the shortage of the load situations before the attack. In the other words, cloudlets have the minimum value of the bandwidth at these frequencies and either have normal or overload at other points. After performing the attack, the cloudlet's bandwidth reaches its minimum loading at frequencies equal to 0.0883, 0.194, 0.25, 0.333, 0.444 & 0.5 Hz. According to the critical frequencies, it is seen that the frequencies equal to 0.0883, 0.444 & 0.5 Hz is common before and after the attack. So, we could say these frequencies are not affected by the attack. This way, it is concluded that the attack has destroyed the frequencies equal to 0.278 & 0.361 hertz and has created the new ones equal to 0.194, 0.25 & 0.333 hertz.

According to the given explanations, the attack source has changed the behavioral pattern of the bandwidth of the cloudlets.

C. Comparing the cpu output variations versus time

Figure 5 shows the CPU utilization by the victim cloudlet before and after the attack.



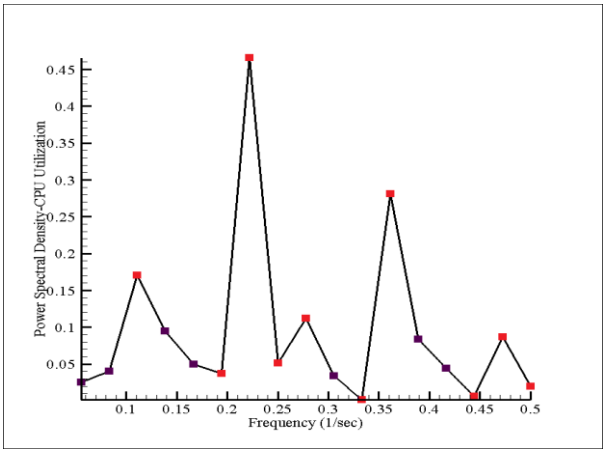


Fig. 5. The diagram of CPU utilization by the victim cloudlet before (up) and after (down) the attack

Regarding to the figure 5 the frequencies equal to 0.139, 0.294, 0.305, 0.388 & 0.472 Hz are representatives of the overload situations before the attack. In the other words, cloudlets have the maximum value of the CPU utilization at these frequencies and either have normal or shortage of the utilization at other points. After performing the attack, the cloudlet's CPU utilization reaches its maximum loading at frequencies equal to 0.111, 0.222, 0.277, 0.361 & 0.472 Hz. According to the critical frequencies, it is seen that the frequency equal to 0.472 Hz is common before and after the attack. So, we could say this frequency is not affected by the attack. This way, it is concluded that the attack has destroyed the frequencies equal to 0.139, 0.194, 0.305 & 0.388 hertz and has created the new ones equal to 0.111, 0.222, 0.277 & 0.361 hertz.

Furthermore, regarding to the figure 14 the frequencies equal to 0.0883, 0.167, 0.277, 0.361, 0.444 & 0.5 Hz are representatives of the shortage of the load situations before the attack. In the other words, cloudlets have the minimum value of the CPU utilization at these frequencies and either have normal or overload at other points. After performing the attack, the cloudlet's CPU utilization reaches its minimum loading at frequencies equal to 0.0883, 0.194, 0.25, 0.333, 0.444 & 0.5 Hz. According to the critical frequencies, it is seen that the frequencies equal to 0.0883, 0.444 & 0.5 Hz is common before and after the attack. So, we could say these frequencies are not affected by the attack. This way, it is concluded that the attack has destroyed the frequencies equal to 0.167, 0.278 & 0.361 hertz and has created the new ones equal to 0.194, 0.25 & 0.333 hertz.

According to the given explanations, the attack source has changed the behavioral pattern of the CPU utilization of the cloudlets.

The frequency in the presented diagrams is the representative of the time step between dominant cloudlet's behavioral patterns. For example the frequency equal to 0.139 hertz for the overload situation before the attack, is shown that the cloudlet's bandwidth utilization reaches its maximum every (1/0.139) 2.12 seconds.

VII. CONLUSION

The main objective of this research is to simulate the resource freeing attack using cloudsim simulator and interpreting the victim and attacker cloudlets behavior. This way we could discuss the attacker cloudlet's behavior and interaction with other cloudlets. Regarding to the mentioned explanations and compairing data before and after the attack, we could found some properties of the attack as follows:

1.Occurrence of the attack would change the consumption pattern of the victim resource.

2.Occurrence of the attack would change the consumption pattern of one other resource at least.

3.After the attack, one of the resources would become the crisis of the system at least.

4.The attack would either change the pattern of two resources or make one of the resources to the crisis.

In the future researches we will present a method in order to prevent this attack and some other methods for detecting and opposing it

Acknowledgment

Here is where I have to thank Mr. Saber Mohammadi who helped out in many aspects of this project.

References

[1] VMWare. [Online]. http://www.vmware.com/

[2] Menascé.,D.A. "Virtualization: Concepts, applications, and performance modeling," in International CMG Conference, 2005.

[3] Devi.,K. , Sujan,.R. ., P.G. , Student,. ,Nadu,S. "A Survey on Application of Cloudsim Toolkit in cloud computing",International Journal of Innovative Research in Science, Engineering and Technology (An ISO 3297:2007 Certified Organization) Vol.3 ,Issue 6, June 2014

[4] Adam.,B. , Mood.,R. , Platcher.,J. , Pruse.,H. , Valafar.,M. , Bulter.,K. , "On Detecting Co-resident Cloud instances using network flow watermarking techniques" Int . J,Inf.Secur . (2014).

[5] Barham.,P. ,"Xen and the art of virtualization," ACM SIGOPS Operating Systems Review, vol. 37, no. 5, pp. 164-177, 2003.

[6] Kazi,S., Aunnurhain , vrbsky ,"Security In Cloud Computing", University of Albama ,2009, vol 2

[7] Harauz, J., Kaufman, L., M,potter,B.,"Data Security in the World of Cloud Computing" , published by the IEEE Computer and Reliability Societies, JULY/AUGUST 2009

[8] Calheiros , R. N . , Ranjan, R.,Beloglazov, A.,De Rose, C.A.F., Buyya,R."
Cloudsim :a Toolkit for modeling and simulation of cloud computing environments and evaluation of resource provisioning algorithms" SOFTWARE- PRACTICE AND EXPERIENCE softw. Pract. Exper. 2011.

[9] Armbrust M, Fox A. , Griffith R. , Joseph A. , Katz R. , Knowinski A. , Lee
G, Patterson D. , Rabkin A. , Stoica I ,Zaharia M. A view of cloud computing.Communications of the ACM 2012;53(4):50-58

[10] Varadarajan, V., Kooburat, T., Farley,B., Ristenpart ,T.and Swift,M.M.,
"Resource-Freeing Attack : Improve Your Cloud Performance" In Conference on Computer and Communications Security 2012.

[11] Barker , S.K. , Shenoy, P.," Empirical evaluation of Latency Sensitive application performance in the cloud " , In MMSys , 2010.