International Journal of Engineering Research and Development
e-ISSN: 2278-067X, p-ISSN: 2278-800X, www.ijerd.com
Volume 12, Issue 8 (August 2016), PP. 27-33

Intrusion Tolerance System Using VM Balancing In Virtual Environments

Hyun Kwon andYongchul Kim
Department Of Electrical Engineering, Korea Military Academy

Abstract:-Computing systems that provide useful services to clients are connected to the Internet. Unfortunately, there are malicious clients who make them susceptible to attacks. Even though security solutions such as an intrusion prevention or firewall can be used to protect such attacks, it is not always possible to defend systems against attacks completely. The studies on intrusion tolerant system (ITS) have been proposed to maintain the proper services in threatening environments. In this paper, we propose an ITS using VM balancing scheme which can balance online virtual machines within each of hosts. The proposed method reduces the damage of VM escape that allows an attack to move from one virtual machine to another virtual machine in a host. By this method, the proposed scheme can guarantee the minimum of services to clients, even under malicious intrusion such as VM escape.

Keywords:-Intrusion Tolerance System, VM balancing, SCIT (Self Cleansing Intrusion Tolerance), VM

I. INTRODUCTION

In the modern warfare, collecting information and real time decision-making are very important. Hence, an automated command and control system is considered as a key factor in the whole process of war. Even if the command and control system has been developed for secure data exchange, a server that has confidential information is attacked by enemy, which leads to a negative consequence. Recently,cyber attacks that are targeting government control system as well as personal information are significantly increased.One of the well-known solutions for the cyber attack is a cryptography technique [1] that is a method of storing and transmitting data using encryption and decryption process. Moreover, intrusion defense system (IDS) and intrusion prevention system (IPS) are used against cyber attacks [6]. However these solutions are limited to thoroughly prevent cyber attacks since the pattern of attack is distributed and stealthy. Zero day attacks that target publicly known but still unpatched vulnerabilities are also difficult to be detected. Therefore, the perfect defense system against every cyber attacks can not be existed.

In recent years, many researchers are studying on intrusion tolerance system (ITS) [1] [2] [6]. The main goal of this system is to provide normal service even under the situation of attack. Cloud computing environment and virtual machine (VM) techniques have been involved in developing effective intrusion tolerance system. One of the well known ITS is self cleansing intrusion tolerance (SCIT) system, which is using VM snapshots to recover system periodically, hence the exposed time to an attacker will be reduced. Figure 1 shows a structure of SCIT in virtual environment and VM rotation. There are several hosts under a central controller and every VMs in each host are controlled by the central controller. Each VM undergoes periodic cleansing as directed by the controller; the cycle of a service is Active – Grace period – Cleansing – Live spare. Active state indicates the service becomes online to receive and process incoming requests, thus the active state period is called SCIT exposure window. Grace period means the service stops accepting new requests and tries to complete the requests in its queue. Cleansing state is that the service is offline and undergoes the restoration cleansing to a good state. Live spare state is the service is in ready but still offline. If we use a notation of Mean Time To Security Failure (MTTSF) as the reliability of a service operating in the presence of cyber attack, it is clear that the less the exposure window the longer the MTTSF [2].

The SCIT related studies mainly focus on reducing exposed time by cleansing VMs in every host to minimize the damage in each VM. However they do not consider the case where some of the hosts can beshut down by a special attack pattern such as VM escape attack [3]. Therefore, in this paper we propose a new SCIT system that mitigates the damage from the host attack by using VM balancing scheme in the virtual environment.

The rest of this paper is organized as follows. In the next section, we discuss related work. In Section III,we propose a new SCIT system that is based on VM balancing. The performance of proposed system and analysis are shown in Section IV. Section V concludes the paper.

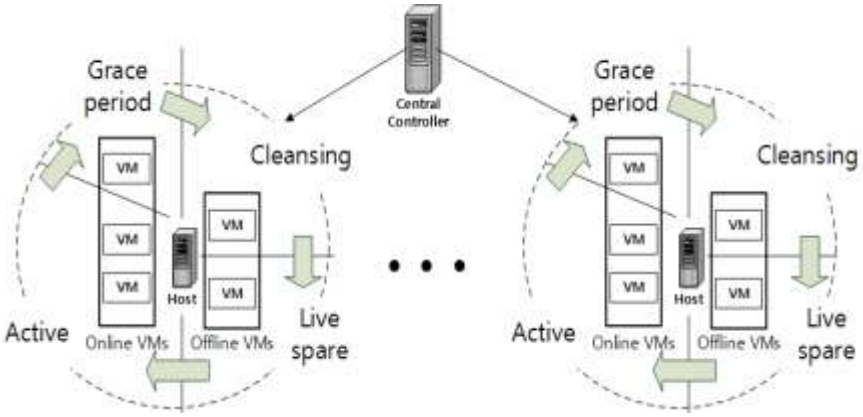

Fig.1:VM rotation[2][11]

II. RELATED WORKS

Cluster is a group of VMs that provide services to clients. Huang [7] presents a structure of an cluster as shown in Figure 2. Every VM keeps swapping of service instances by the controller. The link between live spare state VM and the controller is two-way communication, but the link between active state VM and the controller is only one-way communication to prevent any potential hacker coming through the online VM.

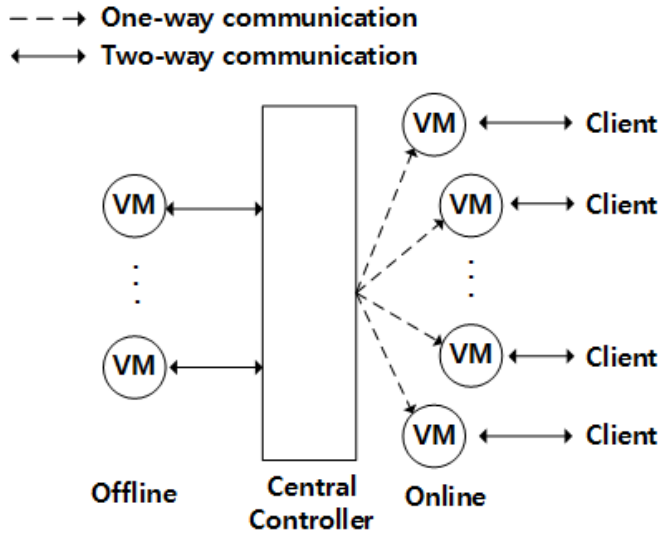

Fig. 2:SCIT cluster architecture

Lim [8] introduced adaptive cluster transformation (ACT) based ITS, which is controlling the number of VMs according to the amount of current requests. The structure of ACT based ITS is shown in Figure 3. This scheme can secure the performance of a system under a massive packet attack such as DoS (Denial of Service). However it requires unlimited VM resources. Lim presents another work [9] that preserves system performance under the limited VM resources by increasing the exposed time of active state instead of extending cluster size. Hybrid Recovery-Based ITS was introduced in [10]. This scheme reactively controls the exposed time of VMs with an expectation of the attack patterns.

Most of the related works above focused on maintaining service performance under a massive cyber attack, and made an effort to protect VMs from the attacks. Hence none of the previous works considered the damage of a host that has multiple VMs. In recent computer security, VM escape is known as the process of breaking out of a virtual machine and interacting with the host operating system [3]. If only one VM is attacked, then the rest of VMs will be affected as long as they are online in the same host. Figure 4 shows an example of VM escape attack.

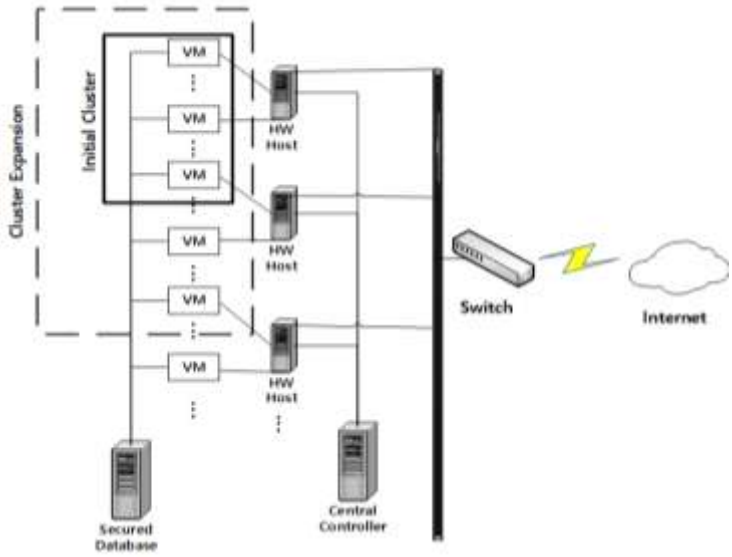

Fig. 3:ACT architecture

In a conventional SCIT system, the number of VMs in a host varies all the time. When a host has many active state VMs compare to the other hosts, the overall performance of the SCIT system will be lower due to the slow data processing time in a busy host. To improve the whole system performance, VM's migration scheme is introduced in [4]. The number of active state VMs in each host is uniformly distributed by actual moving from host to host. We use this load balance concept in a proposed SCIT system to mitigate the damage from VM escape attack, thus the required minimum services can be maintained even if one of the hosts is attacked. However we do not allow VMs to move from host to host in order to provide more fast and efficient services to clients. The detail process of the proposed SCIT system will be addressed in the next chapter.

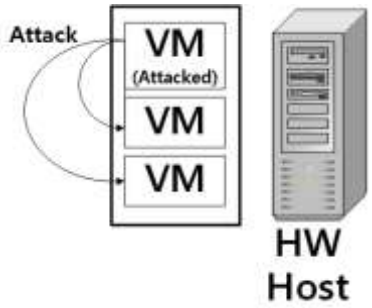

Fig. 4: An example of VM escape

III. PROPOSED SCIT SYSTEM

All paragraphs must be indented. All paragraphs must be justified, i.e. both left-justified and right-justified.Conventional SCIT system focuses on controlling the exposed window period of each VM to prevent possible cyber attacks. In other words, conventional SCIT system is a proactive recovery based system that tolerates intrusions by reducing the exposed time of VMs.Since the load balancing idea was not taken into account in a conventional SCIT system, if a host is attacked by the VM escape attack, then the whole system may not be functioning properly. For example, if we assume that the minimum level of service requires three online VMs in a system where two hosts A and B are having four VMs respectively. At the specific time where four VMs are online in host A and only two VMs are online in host B, if host A is attacked by VM escape then the total number of active state VMs are only two, which is lower than the required minimum level of service. To avoid this situation, our proposed SCIT system ensures that the number of online VMs in each host is more or less equally distributed by the central controller, hence the required minimum level of service is likely to be satisfiedunder the VM escape attack. Figure 5 shows architecture of the proposed SCIT system.VMs in each host divided into two groups. One is online VMgroup that is active state to provide services to clients and the other is offline VM group that is live spare state and ready to be replaced with online VM.

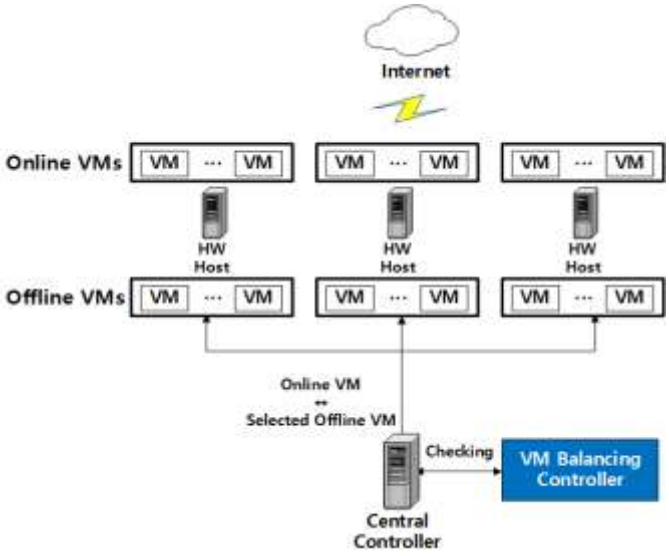

Fig. 5: Proposed architecture

The central controller is responsible for switching online and offline VMs in each host. Whenever the exposed window period of an online VM in any host is expired, the central controller send that VM into the offline group in the same host to be recovered.Instead, the other VM that is already recovered and waiting to be active will be sent to the online group in that host by the central controller. In our system we use another controller, called VM balancing controller, for counting the number of online VMs in each host and determining which VM should be switched first to keep the balance between the hosts. This information from the VM balancing controller is provided to the central controller to for keeping the balance in the whole system.

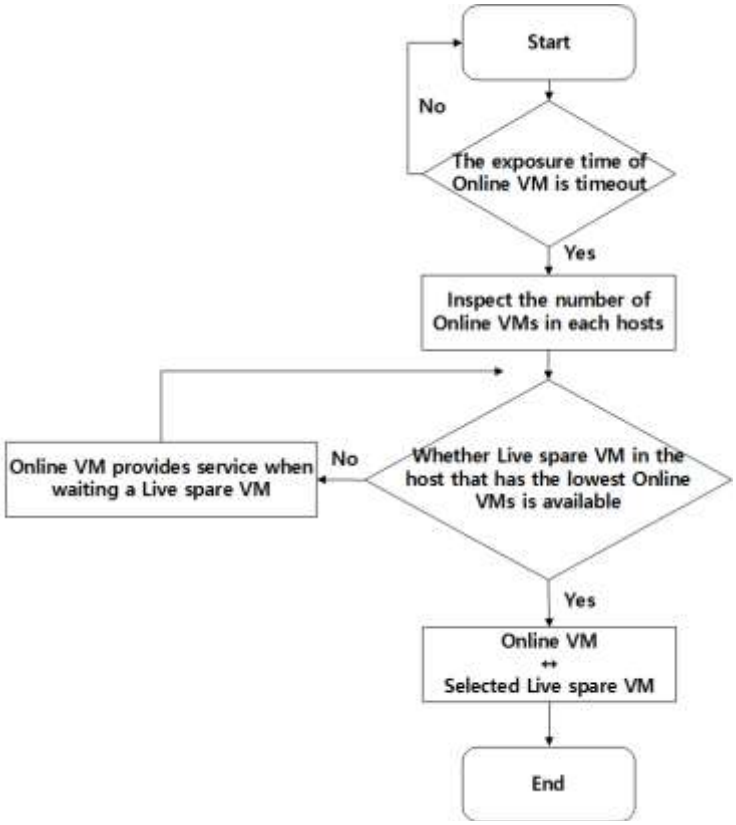

Fig. 6: Flow chart of the proposed algorism

Figure 6 shows aflow chart of the proposed algorism. Whenever the exposure time of online VM in any host is expired, the system starts counting the number of online VMs in each host. Then the host that has the

lowest number of online VMs is selected to see if it has live spare state VMs available. If yes, one of the live spare state VMs will be switched with the expired online VM in the same host. If not,the expired online VM will be extended to provide service until the live spare VM is available in that host. Therefore, switching VMs from different hosts is not allowed in the proposed system.

We describe this algorism through an example.

Example: Consider a simple system with three hosts and each host has four VMs as shown in Figure 7. When an exposure of an online VM in host 3 is time-out, it is clear that one of the live spare state VM should be replacedand take over the expired VM's service. In case a conventional SCIT system is applied in this scenario, one of the live spare state VM will be randomly chosen to be replaced. In Figure 7, there are two live spare state VMs are possible to be chosen, one is in host 1 and the other is in host 2. If the one in host 1 is randomly chosen to be active state VM, then the number of online VMs in host 1 becomes four while the host 2 and host 3 have two online VMs respectively as depicted in Figure 8. Therefore, the vulnerability of VM escape attack increases significantly. Half of online VMs will be disabled when host 1 isaffected by the VM escape attack. In contrast to the conventional system, the focus of our proposed scheme is to preserve the balance such that every host maintains more or less same number of online VMs all the time. In case our proposed scheme is used in the above example, the VM balancing controller will pick up the live spare state VM in host 2 for the purpose of preserving balanceas shown in Figure 9. Thus, thevulnerability of the VM escape attack is minimized and it is guaranteed that more than half of online VMs are always operating even if one of the hosts is attacked.

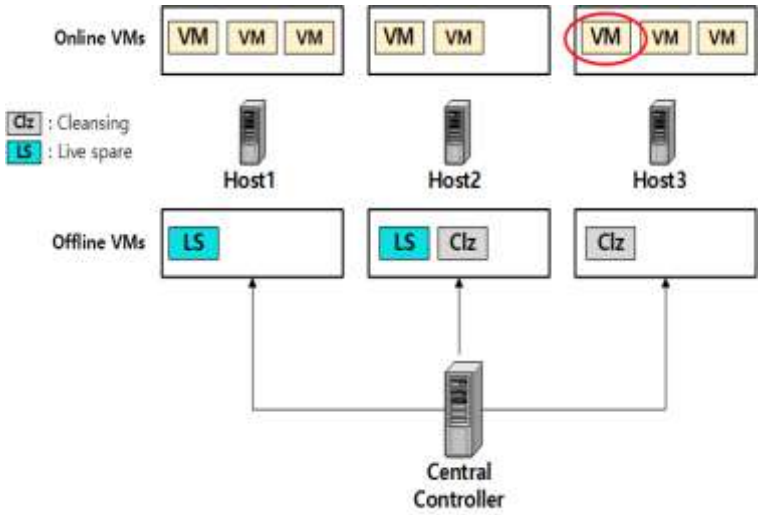

Fig. 7: Example of a system with three hosts and each host has four VMs

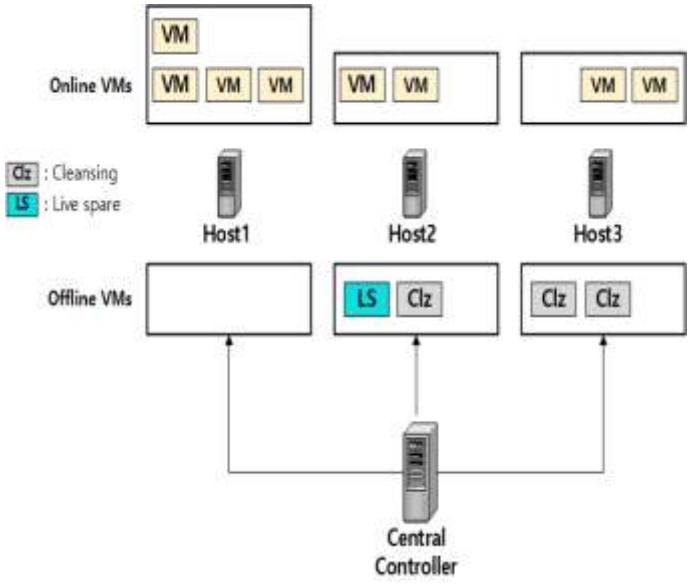

Fig. 8: An example of a conventional SCIT applied in Fig .7

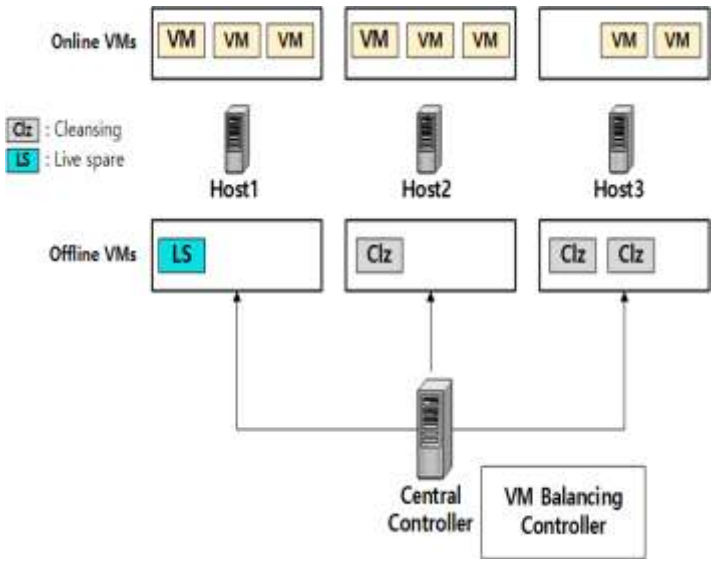

Fig. 9: An example of the proposed scheme applied in Fig.7

Table. 1: An experimental environment and values

Parameters	Contents and values
W_O	The exposure time of online VM : 3 minute (180seconds)
$T_{Cleansing}$	Cleansing time : 1minute (60seconds)
n	The total number of online VMs : 8
N	The total number of VMs : 12
H_t	The total number of VMs in each host : 4
n_h	The total number of hosts : 3
Ω_{min}	The minimum level of service : 5 online VMs

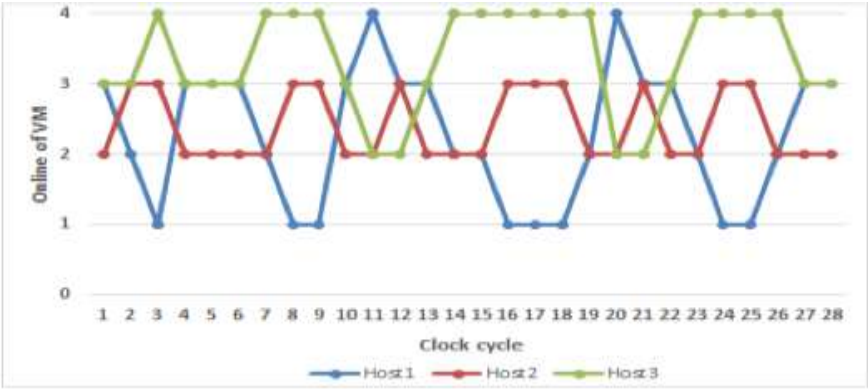

Fig. 10: Number of Online VM as a function of clock cycle with a conventional SCIT

IV. PERFORMANCE ANALYSIS

In this section, the performance of the proposed scheme is compared with a conventional SCIT scheme by using Cloudsim simulator [5]. The experimental environment andvalues used for the simulation are listed in Table 1.The considered system consists of three hosts and four VMs are assigned in each host. The required number of online VMs from the perspective of users is eight and the minimum level of service requires five online VMs. The same experimental environment is applied for both conventional and proposed system.

Figure 10 shows the number of online VMs as a function of clock cycle for different hosts in conventional system. Whenever one of the online VMs is recovered, clock cycle is increased by one. Cloudsim simulation runs during 100 thousand packets are processed. The number of online VMs in one host reaches four in many times especially when the clock cycle is 3, 7~9, 11,14~20, 23~26. During these periods the vulnerability of an attack is serious. If a VM escape attack happens during these periods, the total number of online VMs in the system will be lower than the minimum level of service. In other words, approximately 57% of the whole period is vulnerable to an attack and does not provide the minimum level of service. On the other

hand, as shown in Figure 11, when the proposed scheme is applied, most of the time the number of online VMs in each host remains two or three throughout the simulation. Only a few times there are four online VMs in one host during especially when the clock cycle is 3~5, 13~15, 28, 32. It is certain that the proposed SCIT system minimizes the damage from the possible VM escape attack by using VM balancing scheme. In other words, the proposed system provides minimum level of service even under the VM escape attack situation.

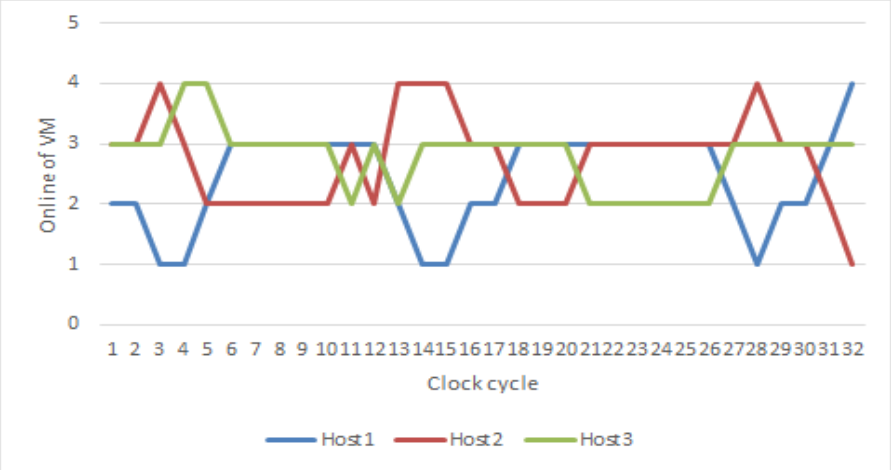

Fig. 11: Number of Online VM as a function of clock cycle withthe proposed scheme

V. CONCLUSION

As the demand for protecting information and communication system of government organization increases, provisioning of security solutions becomes more important. One of the most widely discussed approaches in the research is the SCIT system, which is using VM snapshots to recover system periodically. In this paper we show that the SCIT system is vulnerable to acertain attack such as VM escape attack. To minimize this vulnerability we proposed a VM balancing based SCIT system. The simulation results show that the number of online VMs in each host is uniformly distributed under the proposed system, therefore the damage from the malicious VM escape attack can be mitigated and the minimum level of service can be guaranteed all the time.

REFERENCES

[1]. Kwon, Ohmin, et al, "A Survey on Intrusion-Tolerant System," Korea Computer Congress 2012, 2012.
[2]. Q. Nquyen, and A. Sood, "Quantitative Approach to Tuning of a Time-Based Intrusion-Tolerance System,"Portugal : 3rd Workshop on Recent Advances in Intrusion Tolerance System, 2009.
[3]. Kanika, "Analysis of Virtualization : Vulnerabilities and Attack over the Virtualized Cloud Computing," International Association of Scientific Innovation and Research (IJETCAS), 2014.
[4]. Wilcox Jr, "Dynamic load balancing of virtual machines hosted on Xen," Master's Thesis. USA : Brigham Young University, 2009.
[5]. Rodrigo N. Calheiros, "CloudSim: a toolkit for modeling and simulation of cloud computing environments and evaluation of resource provisioning algorithms," SOFTWARE – PRACTICE AND EXPERIENCE Softw. Pract. Exper. p 23–50, 2011.
[6]. Heo, Seondong, et al, A Survey on Intrusion-Tolerant System," Journal of Computing Science and Engineering (JCSE). p 242-250, 2013.
[7]. Huang, Yih, David Arsenault, and ArunSood, "Closing cluster attack windows through server redundancy and rotations," Sixth IEEE International Symposium on. Vol. 2. IEEE : Cluster Computing and the Grid 2006 (CCGRID 06), 2006.
[8]. Lim, Jungmin, et al, "A novel Adaptive Cluster Transformation (ACT)-based intrusion tolerant architecture for hybrid information technology," The Journal of Supercomputing 66.2. p 918-935, 2013.
[9]. Lim, Jungmin, et al, "The Design of a New Virtualization-Based Server Cluster System Targeting for Ubiquitous IT Systems," Springer Netherlands : Ubiquitous Computing Application and Wireless Sensor. p 361-375, 2015.
[10]. Bumsoon, J.A.N.G, et al, "Hybrid Recovery-Based Intrusion Tolerant System for Practical Cyber-Defense," Institute of Electronics, Information and Communication Engineers (IEICE) TRANSACTIONS on Information and Systems 99.4. p 1081-1091, 2016.
[11]. Nguyen, Quyen L., and ArunSood, "Designing SCIT architecture pattern in a Cloud-based environment," IEEE/IFIP 41st International Conference on IEEE : Dependable Systems and Networks Workshops (DSN-W), 2011.