Security-Aware Dispatching of Virtual Machines in Cloud Environment

Mohammad Amin Keshtkar[1], Seyed Mohammad Ghoreyshi[2], Saman Zad Tootaghaj[3]

Electrical and Computer Engineering Department, University of Tehran, Tehran, Iran
[1]a.keshtkar@ut.ac.ir
[2]m.ghoreyshi@ece.ut.ac.ir
[3]s.tootaghaj@ut.ac.ir

Abstract

The cloud computing as a ubiquitous paradigm could provide different services for internet users and Information Technology (IT) companies through datacenters located around the world. However, cloud provider faces several problems such as security and privacy issues in cloud datacenters. Hence, cloud provider has to handle security challenges to gain more profit. In this paper, a Security-Aware Dispatching and Migration model for the virtual machines is proposed in order to prevent Service Level Agreement (SLA) violation. The approach considers the lowest violation in required security preservation as the most significant factor for execution of VMs. The results show that lower SLA violation is achieved in our method compared to other common methods. It is also shown that the SLA Violation has an exponential relationship with the VM computational capacity which is defined by Million Instructions Per Second (MIPS).

Keywords: *Cloud computing, Security Provisioning, Dispatching, Online Migration*

1. Introduction

Cloud computing as a ubiquitous paradigm offers scalable on-demand services to users through various datacenters (DCs) located around the world with greater flexibility and lesser infrastructure investment [1,2]. Users anywhere in the world can access anything as services such as infrastructure, platform, and software from the cloud and pay for only the service they use. Also IT companies can benefit from this new paradigm by eliminating the need to maintain an in-house datacenter by migration of their own data to a cloud datacenter [3].

On the other hands, security and privacy issues are the greatest concern for cloud providers and the biggest challenge for the adoption of Cloud. To solve these problems, applying the security-aware techniques is vital for the cloud providers. Users have different concerns about security and privacy of their data. As a result, the public adoption of cloud services will be depended on the desirable security needs of companies and users; and abilities of cloud provider to satisfy them [4,5].

Service Level Agreements (SLA) is a contract negotiated and established among users and cloud provider that formalize performance metrics and QoS parameters such as deadline, throughput, response time or latency. Also, Cloud service providers often establish a Service Level Agreement to highlight security and privacy issues of the submitted services. For instance, when users submit their application with different security level constraint to the system, they expect that system is able to meet their security constraints with maximum success probability [6]. For this reason, we proposed a security-aware algorithm in cloud environment to reduce security violation in dispatching of submitted VMs. Moreover, security-aware migration of virtual machines is another way to reallocation of VMs based on the security constraints in our proposed method. Another application of VMs migration is that VMs can be consolidated to minimize number of physical machines (PMs) and idle PMs can be turned off subsequently [7].

In this paper, in order to satisfy security requirements of submitted VMs in cloud environment, we propose a Security-Aware Dispatching model and security-aware migration of virtual machines between physical machines by considering variation in security levels of VMs. We consider SLA Violation when a submitted VM cannot run on a desirable physical machine from security aspects.

The remainder of this paper is organized as follows: we address the related work in section 2. The system model including Datacenters model, virtual machines model, security model are described in Section 3. The Heuristic algorithm is presented in section 4. Then Experimental results are provided in Section 5. Finally, Section 6 concludes the paper.

2. Related Work

In [8], authors explain the new risks that face administrators and users of a cloud's image repository. To address these risks, they propose an image management system that controls access to images.

Ning Cao in [9], defined and solved the challenging problem of privacy-preserving multi-keyword ranked search over encrypted cloud data and establish a set of strict privacy requirements for such a secure cloud data utilization system to become a reality. Also in [10], a large amount of research work has dealt with the characterization of cloud computing and an efficient privacy preserving keyword search scheme in cloud computing is proposed.

In [11], authors describe how the combination of existing research thrusts has the potential to alleviate many of the concerns impeding adoption to cloud. The paper [12] introduces a Trusted Third Party, tasked with assuring specific security characteristics within a cloud environment.

In [13], PasS (Privacy as a Service) has been presented as a set of security protocols for ensuring the privacy and legal compliance of customer data in cloud computing architectures. S.pearson in [14], describes a privacy manager for cloud computing, which reduces the risk to the cloud computing user of their private data being stolen or misused, and assists the cloud computing provider to conform to privacy law.

In [15], authors seek to begin the process of designing data protection controls into clouds from the outset so as to avoid the costs associated with bolting on security as an afterthought. In [16], authors investigate the complex security challenges that are introduced by the trend towards Infrastructure as a Service (IaaS) based cloud computing.

3. System Model

In this paper, several physical machines distributed in the one cloud datacenter are described. As depicted in Fig (1), the Security-Aware Dispatcher acts as an interface between physical machines and cloud users.

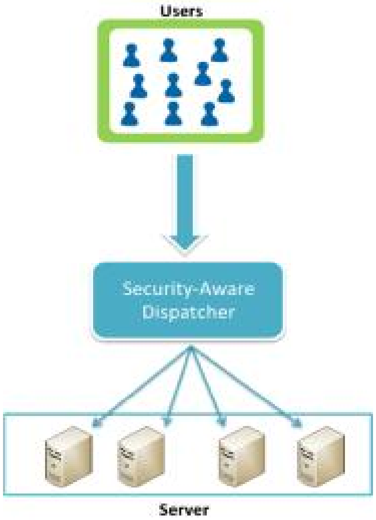

Fig.1 Security-Aware Dispatcher Model in cloud datacenter

The Security-Aware Dispatcher must distribute VMs among physical machines based on parameters like Security and Performance. It is assumed that physical machines are homogeneous with respect to the computational capacity. Each physical machine has a local manager in order to handle the running and migration of VMs. The local manager monitors the execution of VMs and issue orders for VM migrations. A submitted VM could be easily migrated between different physical machines by assuming that there is network connection between for each pair of physical machines. Also, the approach of this paper considers the time delay caused by the network in the used VM migration timing model.

3.1 Jobs and Virtual Machines Model

Users submit their VMs to the Security-Aware Dispatcher with a security requirement parameter. In this model, each VM has a specific security-level that should be satisfied by the cloud provider. Furthermore, each job has a specific execution time and computational capacity such that each VM is modelled as the following:

$$VM_i(t_i, m_i, s_i, r_i), \quad (1)$$

where t_i and m_i indicate the execution time of i^{th} VM and computational capacity (MIPS) of submitted VM, and in this model r_i and s_i represent the amount of requested RAM and the Security-Level of i^{th} VM, respectively. These virtual machines must meet the Security-Level constraints of the cloud users.

3.2 Security Model

Since security attacks frequently occur in a cloud environment, the continuous monitoring of VMs is indispensable. After the first allocation of VMs between physical machines, the local manager should check out the status of VMs for their security conditions. In this paper, we consider that each server configured with different security characteristics. The dispatching that is unaware about security could lead to disastrous results in cloud datacenters. The local managers must monitor the security of VMs continuously and manage the VMs according to their security needs in order to prevent critical information being attacked by malicious insiders. Moreover, when some processors are released by their VMs, local managers should inform the Security-Aware Dispatcher that their physical machines are ready to accept new VMs. Then, Security-Aware Dispatcher is able to migrate VMs between physical machines in order to gain higher security level for running VMS. Consequently, VMs could be migrated to another available physical machine to enhance the total security of cloud datacenter.

4. Heuristic Algorithm

Our goal in this paper is introducing an approach for allocating VMs to the physical machines and then monitoring their running status and handling security attacks that may be occurred for them. First, users submit their VMs with their requirements to the Security-Aware Dispatcher. The Security-Aware Dispatcher sort VMs and physical machines based on their security-level into decreasing order in separate lists. Then, Dispatcher takes the VMs from the VM's lists and assign each one to the first server in the server's list with adequate computational capacity.

This algorithm could provide a fast solution, involving placing each VM into the first physical machine in which it will fit. It requires **Θ**(n log n) time, where n is the number of VMs to be assigned. The algorithm was improved by first sorting the list of VMs into decreasing order (sometimes known as the first-fit decreasing algorithm).

The Dispatcher could distribute virtual machines among physical machines based on their required MIPS and security-levels. The main goal of the Security-Aware Dispatcher is allocating each virtual machine to a physical machine in the cloud environment that could schedule assigned VM and has minimal violation in the security provisioning. In order to schedule virtual machines on each physical machine, the following conditions should be met [6]:

$$\sum m_k \leq PM_{cap}, \qquad (2)$$

where PM_{cap} represents processing capacity of each physical machine. This means that multiple virtual machines could be allocated to each physical machine if their total required MIPS be less than physical machine capacity.

Unfortunately, due to insufficient available resources in the cloud datacenters, the initial allocation through the Dispatcher would not be efficient during the running time. Hence, local managers must constantly monitor the completion time of virtual machines to be able to act an appropriate response for efficient reallocation. After completion of VMs, their computational capacity would be released and be available to be used by another VMs. For this reason, in proposed model, VMs could migrate to the physical machine with higher security level which has adequate released computational capacity. The migration time of each virtual machine is calculated according to the amount of RAM of each VM and available bandwidth between physical machines. Hence, VM migration time could be calculated as following:

$$t_{mig} = \frac{r_{vm}}{bw_{ik}}, \qquad (3)$$

where r_{vm} represents the amount of RAM used by the virtual machine. Also, bw_{ik} indicate the amount of available bandwidth between ith and kth physical machines.

5. Experimental Result

5.1 Simulation Setup

In this paper, the CloudSim simulator is used for the simulation of physical machines and cloud environment. To accomplish this, the following components were added to our simulation model:

- Migration of virtual machines between physical machines.
- Physical machines equipped with different security levels.

Several physical machines with different security level included Very Low security levels (1), Low security levels (2), Medium security levels (3), High security levels (4), Very High security levels (5), have been simulated in CloudSim Toolkit. Physical machines are homogeneous with respect to the computational capacity. However the security levels of physical machines are heterogeneous. In this study, five security requirements for each VM are considered. Minimum and maximum security requirement of each VM are considered similar to security levels of physical machines. Also, it is assumed that SLA Violation time is equivalent to the time intervals which VMs are executing on a server that could not satisfy user's expected security level.

The additional assumption is that there is a network connection between each pair of physical machines to migrate virtual machines. Available bandwidth between each of them is selected from the range of 1 Gbit/s to 4 Gbit/s. The cloud provider revenue was set to the subtraction submitted VM profit and SLA Violation Cost in order to compare the proposed algorithms.

The VMs have different security levels, such that, a VM is profitable for the provider when it is executed on the expected secure physical machine in its execution time period. It is assumed that 500 VMs arrive at time 0. The MIPS of each VM is selected randomly from 250 to 1000 and its security level is determined from 1 to 5 randomly. The amount of RAM for each virtual machine is selected between 1000 MB to 4000 MB based on the amount of MIPS that must be supported by them. The computational capacity in physical machines is equal to 1000 MIPS. In this model, after completion some VMs, the Dispatcher compare the security levels between VMs which are running on undesirable physical machines and then select VMs with higher security needs in comparison to others. Afterwards, Dispatcher migrate selected VMs to their appropriate physical machines. We consider that monitoring of VMs completion is accomplished every 5 seconds. In addition, we compared the proposed algorithms based on the SLA violation on different number of submitted VMs.

5.2 Simulation Results

In this paper, we consider two assumptions for evaluation of different proposed methods. First assumption is related to distribution model of VMs. The algorithm employs Security-Aware Dispatching (SAD) if VMs distributed according to their security needs; otherwise, virtual machines are distributed based on the Simple Consolidation Method (SCM) which is non-aware about security. In consolidation method, we sort VMs only based on their computational capacity, and then distribute VMs on physical machines in order to use minimal physical machines. The second assumption is about having or not having VMs migration policy between physical machines. For example, we call Security-Migration (SM) for our policy to migrate VMs based on the security policy and Consolidation-Migration (CM) for migration based on the consolidation policy. Therefore, we name our method SAD-SM. This means that virtual machines are distributed based on the security level of each VM and physical machine and they could migrate between physical machines in accordance with release of occupied resources.

By using several simulations we have shown that SLA Violation of our method significantly is lower than other methods. Comparing our algorithm (SAD-SM) with SCM-CM and SAD without migration is depicted in Fig (2). The vertical and horizontal vectors represent Normalized SLA Violation and VM Numbers, respectively.

SLA Violation in the SCM-CM is higher than our migration method. Because, it is assumed SCM-CM method is non-aware about security issue and only consolidate VMs to the physical machines. But in our method, assigning one VM to each physical machine and migration of VM try to prevent security violation and subsequently reduces SLA Violation. Moreover, it is clear that Security-Aware Dispatching without migration lead to increase inflexibility of the model and hence increase SLA Violation.

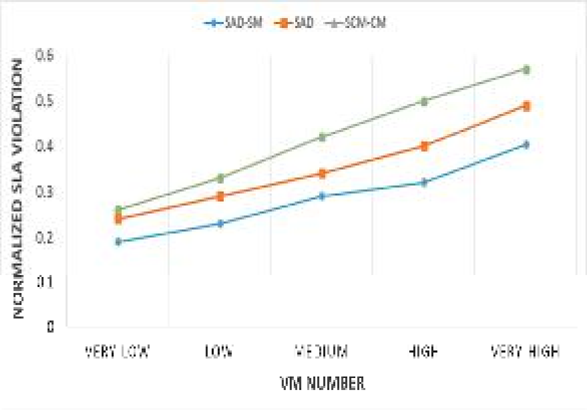

Fig. 2 SLA Violation comparison between different models

In addition, we have evaluated and drawn impact of VM MIPS on SLA Violation in Fig (3). Generally, we changed VM MIPS in order to evaluate impact of VM computational capacity requirements on SLA Violation.

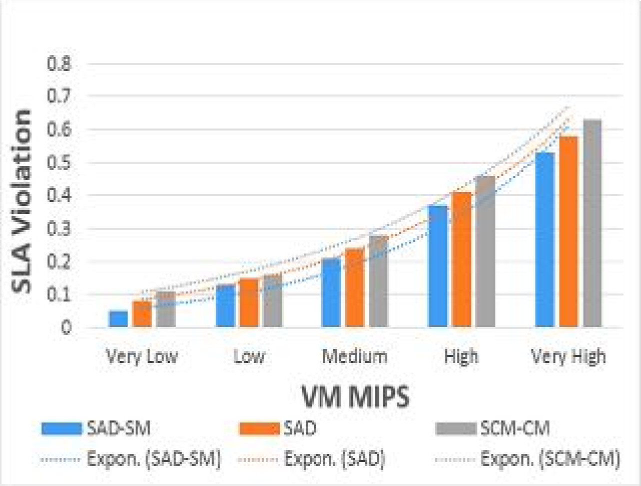

Fig.3 Impact of VM MIPS on SLA Violation

Subsequently, we examined proposed methods in different VM MIPS including Very Low (MIPS=250-500), Low (MIPS=500-750), Medium (MIPS=750-1000), High (MIPS=1000-1250), Very High (MIPS=1250-1500). Clearly, the increase of MIPS lead to decline of available resources in physical machines. As a result, the SLA Violation is increased due to the reducing capacity of high security physical machines and they do not have enough capacity for submitted VMs. As seen in Figure (3), the SLA Violation of proposed methods is increased exponentially with the increase of VM MIPS.

6. Conclusion

The cloud computing in its development way has faced many problems like Security and Privacy issues. Ignoring these problems could lead to disaster in results for cloud provider. So, we proposed a Security-Aware Dispatching and Migration model for virtual machines to manage security needs to prevent SLA violation by considering variation in security requirements. In this paper, we consider the lowest increase in SLA Violation for desirable security of users as the most significant factor for management of each VM. Our method could achieve lower SLA violation compared to other proposed methods. Moreover, we have shown that the increase in VM MIPS has an exponential relationship with the increase in SLA Violation of security in our method.

References

1. Garg, Saurabh Kumar, Chee Shin Yeo, Arun Anandasivam, and Rajkumar Buyya. "Environment-conscious scheduling of HPC applications on distributed cloud-oriented data centers." Journal of Parallel and Distributed Computing vol. 71, no. 6 (2011): 732-749.
2. S. Subashini and V. Kavitha, “A survey on security issues in service delivery models of cloud computing,” Journal of Network and Computer Applications, vol. 34, no. 1, pp. 1–11, Jan. 2011.
3. H. Takabi, J. B. D. Joshi, and G.-J. Ahn, “Security and Privacy Challenges in Cloud Computing Environments,” IEEE Security & Privacy Magazine, vol. 8, no. 6, pp. 24–31, Nov. 2010.
4. Wu, Hanqian, Yi Ding, Chuck Winer, and Li Yao. "Network security for virtual machine in cloud computing." In Computer Sciences and Convergence Information Technology (ICCIT), 2010 5th International Conference on, pp. 18-21. IEEE, 2010.
5. C. Modi, D. Patel, B. Borisaniya, A. Patel, and M. Rajarajan, “A survey on security issues and solutions at different layers of Cloud computing,” The Journal of Supercomputing, vol. 63, no. 2, pp. 561–592, Oct. 2012.
6. D. Svantesson and R. Clarke, “Privacy and consumer risks in cloud computing,” Computer Law & Security Review, vol. 26, no. 4, pp. 391–397, Jul. 2010.
7. B. Hay, K. Nance, and M. Bishop, “Storm Clouds Rising: Security Challenges for IaaS Cloud Computing,” 2011 44th Hawaii International Conference on System Sciences, pp. 1–7, Jan. 2011.
8. Wei, Jinpeng, Xiaolan Zhang, Glenn Ammons, Vasanth Bala, and Peng Ning. "Managing security of virtual machine images in a cloud environment." In Proceedings of the 2009 ACM workshop on Cloud computing security, pp. 91-96. ACM, 2009.
9. N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, “Privacy-preserving multi-keyword ranked search over encrypted cloud data,” 2011 Proceedings IEEE INFOCOM, pp. 829–837, Apr. 2011.
10. Q. L. Q. Liu, G. W. G. Wang, and J. W. J. Wu, “An Efficient Privacy Preserving Keyword Search Scheme in Cloud Computing,” 2009 International Conference on Computational Science and Engineering, vol. 2, pp. 715–720, 2009.
11. Chow, Richard, Philippe Golle, Markus Jakobsson, Elaine Shi, Jessica Staddon, Ryusuke Masuoka, and Jesus Molina. "Controlling data in the cloud: outsourcing computation without

outsourcing control." In Proceedings of the 2009 ACM workshop on Cloud computing security, pp. 85-90. ACM, 2009.

12. D. Zissis and D. Lekkas, "Addressing cloud computing security issues," Future Generation Computer Systems, vol. 28, no. 3, pp. 583–592, Mar. 2012.
13. W. Itani, A. Kayssi, and A. Chehab, "Privacy as a Service: Privacy-Aware Data Storage and Processing in Cloud Computing Architectures," 2009 Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing, pp. 711–716, Dec. 2009.
14. Pearson, Siani, Yun Shen, and Miranda Mowbray. "A privacy manager for cloud computing." In Cloud Computing, pp. 90-106. Springer Berlin Heidelberg, 2009.
15. S. Creese, P. Hopkins, S. Pearson, and Y. Shen, "Data Protection-Aware Design for Cloud Computing Abstract : The Cloud is a relatively new concept and so it is unsurprising that the information assurance , data Data Protection-Aware Design for Cloud Services," no. December, 2009.
16. B. Hay, K. Nance, and M. Bishop, "Storm Clouds Rising: Security Challenges for IaaS Cloud Computing," 2011 44th Hawaii International Conference on System Sciences, pp. 1–7, Jan. 2011.