ISSN 2047-3338

Fair Cloud Management System

Cao Thanh Phuong[1], Dang Thanh Phuc[2], Mai Xuan Phu[3] and Cao Dang Tan[4]
[1,2,3,4]University of Science Ho Chi Minh City, Viet Nam
[1]caophuong2012@gmail.com, [2]dtphuc1302@gmail.com, [3]mxphu@fit.hcmus.edu.vn, [4]tan@hcmus.edu.vn

***Abstract*– Cloud computing offers multiple advantages comparing to "Traditional" computing infrastructures. However, all customer data are stored on a virtual machine (VM) or on a cloud of a service provider (SP). Therefore, service quality and data safety are highly dependent on the SP. It also means that these issues are dependent on SP's privileges on customer's VM. Currently, the rights are not balanced between the SP and the customer on a cloud management system. As a result, the imbalance has granted the SP a number of rights that can cause damage to customer's VM. In such cases, if SP's rights are misused or abused, his customers are highly likely to be adversely affected. To solve this problem, this paper proposed the idea of limiting SP's rights and allowing the customer to prevent the SP from performing dangerous operations on the VM. Our implementation has successfully demonstrated the solution to increase safety for customers while using SP's service. Therefore, the SP is able to acquire competitive advantages in his business.**

***Index Terms*– Cloud Computing, Virtualization, Balance of Rights and Cloud Management System**

I. INTRODUCTION

A permission is an authorization to perform an operation on a specific object, such as a VM or a group of VMs. Permission can be granted by a SP or by anyone who has rights to do that. Administrators belong to such kind of people. In a cloud computing system, the privilege of a user is defined by the user permission assignment (UPA) which is differently depending on each cloud management system. The UPAs on current systems do not guarantee the right balance between the SP and his customers. When a SP uses his privileges to misuse dangerous operations, it can harm to VMs as well as have negative effects on his customers. For example, the customer's critical services can be stopped or customer's VMs might be moved or destroyed unexpectedly, which results in the halt of customer service. In addition, if the SP tracks customer's activities on the VM, the customer's privacy will be seriously violated.

In order to properly evaluate the right balance of both sides (the SP and the customer) on a cloud computing system, this paper suggested three criteria.

First, the UPA on a cloud management system should not lead to any conflicts between a SP and his customers. For example, the UPA does not allow the SP to stop a running VM without the customer's approval.

Second, during the period of a service contract, the SP must respect customer's authority on a VM, and cannot arbitrarily perform any operations on the VM that are able to cause harmful effects to the customer. For instance, the cloud management system does not permit the SP to delete customer's VM during this period.

Third, actions performed on customer's VM by the SP are recorded to the system log. It helps the customer track SP's impacts on his VM and monitor his services more obviously.

With these criteria, the authors made a survey of the privileges of the customer and of the SP on cloud management systems. The result of the survey was analyzed to conclude that the UPA on these systems do not guarantee the right balance between the SP and his customers. After that, this paper would then offer a solution for the right balance on cloud computing system. Based on the proposed solution, our implemented system, Fair Cloud Management System (FCMS), has been developed to demonstrate the idea.

II. RELATED WORKS

In reality, VMs can be directly managed within a host by Virtual Machine Monitor (VMM) or within a cloud by Cloud Management System (CMS).

To simplify the demonstration, the authors divide operations on a VM into three groups basing on their effects on the VM:

- Group I: Initialize and destroy VM.
- Group II: Start VM, stop VM, suspend/pause VM, resume VM, reboot VM, shutdown VM, move/migrate VM.
- Group III: List directory, delete file or directory, run software... (Working operations on the VM).

With the three groups, the following part presents the UPA survey on popular VMMs and CMSs. To make this survey more reliable, the authors did not only gather information from the documents, but also implemented VMMs and CMSs on a cloud computing system for testing. The survey focused on finding which groups of rights are assigned to SP and to customer:

A. Virtual Machine Monitor (VMM)

On Microsoft Hyper-V and Citrix XenServer, the SP has privileges to perform all operations from group I, II on all VMs [6]. Therefore, customer's VMs can be damaged by dangerous operations of the SP. He cannot also know which operations performed on his VMs because there is no system log that are available to customers on these systems.

On VMWare ESXi, SP's rights can be limited partly or completely. The VMWare ESXi provides three default roles [4]:

- No access: A permanent role assigned to new users and groups. It prevents a user or a group from viewing or making changes to VMs. It is equivalent to assigning no role to a user for a particular VM or a group of VMs.
- Read only: A permanent role that permits users to view the status and configuration of VMs without modifying them.
- Administrator: A permanent role that enables a user complete access to all of the VMs on the server. It has all privileges for all VMs on a cloud computing system such as creating and destroying VMs, as well as setting access rights and privileges for users.

The VMWare ESXi has an authorization file [7] that contains information about SP's role corresponding to each VM. On this file, there are parameters that determine the SP's role and the privilege. If SP's role is changed from the Administrator to Read-only or No access, he cannot change the VM state. Thus, the VMWare ESXi theoretically allows limiting SP's privileges on the VM. Nevertheless, this file is stored on a physical machine and is not protected by any security mechanisms, enabling the SP to edit this file to have Administrator role whenever he wants. The VMWare ESXi also does not make a customer possible to track operations performed by the SP on his VMs. In addition, the UPA of VMWare ESXi is not fine enough to adapt many situations in reality.

Overall, the UPA on current VMMs has not satisfied the criteria for balance of rights.

B. Cloud Management System (CMS)

On Citrix XenCenter (XenServer) and VM Manager (Hyper-V), a SP is able to perform all operations from the three groups [1], [3]. The SP can shut down or delete customer's VMs whenever he wants, causing damage to both customer and SP. Moreover, although the actions performed by any users are stored in the system log, the SP is able to clear the event of performed actions. Consequently, the UPA on these CMSs has not met the requirements of the balance of rights.

On vCenter Server (VMWare ESXi), a SP can be limited all rights from the three groups. In particular, vCenter Server provides default roles:

- System roles: With these permanent roles, a user cannot edit his privileges.
- Sample roles: SP/Administrator can modify or remove these roles.

There are three specific system roles:

- Administrator: Allows users to perform all operations from the three groups on all VMs managed by vCenter Server.
- Read-only: Only permits users to view the state and details about the VM such as its current performance and status.
- No-access: Does not let users to perform any operations on VM including viewing VM's status.

In sample roles, user's privileges can be customized while vCenter Server gives a list of operations to assign a user's role. A user can be assigned to a role with no right, with certain rights or with all rights on the VM. The outstanding point of the VMWare ESXi is that the privileges of any users can be restricted [7]. A user assigned to Administrator role can be limited his rights on a specific VM in the cloud system. Therefore, SP's rights can be restricted on customer's VM. It enables the customer to prevent the SP from performing operations on his VMs. However, since the SP have been limited their all rights on a VM, he cannot perform operations to protect his system and the customer's service in case of emergency (e.g., halting a VM that is attacking DOS or is spreading virus to other VMs). This vulnerability might put the whole system and all customers at risk. Therefore, vCenter Server still needs to improve their UPA for its safer and more effective operation.

From these observations, it implies that, on VMMs, only VMWare is concerned about solving the imbalance between SP's rights and customer's rights as it allows putting limitation on SP's rights on a VM. However, as we discussed above, this approach has not completely solved the imbalance of rights between the customer and the SP.

On CMS, only vCenter Server is concerned about limiting SP's rights on customer's VM. Nevertheless, there is nothing to ensure that a VM cannot harm to the whole system, so the SP needs to have a prior privilege to protect his system in the case of emergency.

In the future, when cloud computing becomes more popular, the built-in balance of rights will play a very important role to secure the service of both sides and it helps customers feel safer while using SP's service. Therefore, this paper will then discuss about a solution to solve the imbalance of rights on cloud computing system.

III. SOLUTION FOR BALANCE OF RIGHTS

First, SP's rights on a VM rented by a customer are restricted, e.g., deleting the VM is not allowed during the period of a service contract.

Second, the cloud management system permits the customer to reject SP's operations on his VMs if necessary. For example, if the SP needs to stop a VM for periodical system backup while customer's VM is being used, he has to announce this operation to the customer. The cloud management system only allows the SP to stop the VM once the customer has accepted this action. Otherwise, the SP must backup his system at a different/another time.

Third, for a more obvious management, cloud system will be equipped with a system log. The system log enables customers to track operations performed on their VMs by the SP.

To implement the above solution, this paper proposed four mechanisms depending on SP's operation on a VM:

- Authorize: The SP is authorized to perform the operation by the customer.
- Notify: The SP is allowed to perform the operation. However, upon completion of operation performed on customer's VM, the system will notify the customer about that operation (via SMS message or email). This mechanism helps the customer monitor the operations performed on his VM in almost real time.
- Notify – confirm: When the SP performs an operation on a VM, information of this action will be sent to the customer. Next, the customer will decide to allow or reject this operation on his VM. The operation is only performed after the customer allowed it.
- Be in emergency circumstances: It is critical that in particular situations, the SP have to perform operations that were limited or not allowed during the period of a service contract, in order to protect his system and customers. For instance, the SP have to stop a VM that is attacking DOS to other VMs, to save his system and to ensure the safety of customer's service. In such cases, the cloud management system will proceed with this mechanism in which the SP's operations are allowed to be performed on VMs. Then, the management system requires the SP to give reasons why he had to perform this operation urgently (e.g., signs of DOS attack). This reason will later serve for the non-avoidance of operation performing on VMs in the system.

To assist the above-described mechanisms, it is advisable that UPA be included in the service contract signed by customer and SP. In particular, every important operation on a VM will be accompanied with information about the right of both sides. This information identifies whether SP is allowed to perform an operation, and which mechanism is applied. Both sides must agree on all terms in the service contract before the delivery of the VM to customers. The table below provides the information of the UPA in the service contract:

Table 1: UPA in the service contract

Operation	PMA	VMA
Install OS on VMs	✓	×
Delete VM	×	×
Remove virtual hard disk	×	×
Start VM	Authorized	✓
Suspend (pause)	Notify – confirm	✓
Resume VM	Authorized	✓
Reboot VM	Notify	✓
Shutdown (Power off)	Notify – confirm	✓
Console interaction	×	✓

Note: × not allowed to perform
✓ allowed to perform

A cloud computing system should be managed by CMSs whereas VMMs are only used for initial configurations/installations. In addition, the CMSs can manage the cloud system with many physical machines as VMM can only manage VMs on one physical machine. For these reasons, the authors decided to implement the above mechanisms on CMS to build up the FCMS and on VMM should be implemented similarly.

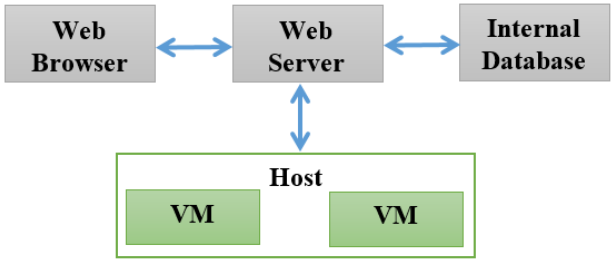

Fig 1: The model of FCMS

Roles of elements:

- Web Browser: The platform on which users (including customer and SP) work with Hosts or VMs.
- Web Server: Receives and proceeds requests from users, serves for communication among web browser, internal database, web browser and Hosts/VMs.
- Internal Database: Contains service contracts, user accounts and system logs.
- Host: Provides resources for virtualization.
- VM: Virtual machine.

The final part of this section describes how the FCMS operates when SP performs an operation on VM.

In the event that it is not an urgent necessity, the web server will transfer the operation to system's database. The database will then identify the corresponding mechanism to this operation. As mentioned above, there are three non-emergency mechanisms:

- Authorize: Database orders web server to transmit the operation to Host and then it will be performed on the VM. After that, the web server will write this action to the system log.
- Notify: Database also tells web server to allow the operation to be performed on the VM. After that, the web server sends an SMS/email to the customer to notify him about the performed operation. Finally, web server will write the information to the system log.
- Notify – confirm: Database requests web server to send an SMS/email to customers to notify him about the operation. The web server will not transmit the operation to the VM until the customer accepts it. This action will be also written to the system log.

In case of emergency, the web server requires the SP to give a reason. The reason given by the SP is recorded to the database and it will be used when the customer needs to know why the operation was performed on his VM. After that, the operation will be performed on the VM without checking the corresponding mechanism in the database.

The FCMS, a cloud management system based on web, is implemented to demonstrate the above solution. It was built by using XenServer APIs [2], [8]. It allows users to perform operations on the three groups on VMs in a Citrix host.

IV. EVALUATION

As mentioned in the section two, VM Manager and Citrix XenCenter do not allow limiting SP's rights on VM. On the contrary, the implemented FCMS does not only allow limiting SP's rights on VMs, but also notifies customers about SP's operations on their VMs.

In comparison with vCenter Server, as the vCenter Server does not allow SP to perform operations after his rights were limited, our FCMS gives the SP a prior privilege to protect his system and customers in case of emergency.

Our implementation also has advantages as compared to VMWare ESXi. Since the VMWare ESXi only has two abilities: no privilege or all privileges; in contrast, our implementation, by using a service contract, allows customers and the SP to make an agreement on any operations they think it is necessary. This flexibility enables the management system adapting to different scenarios in reality and satisfies all customer's requirements.

In conclusion, our FCMS does not only satisfy suggested criteria suggested, but also strengthens the flexibility of cloud system management. With the FCMS, customers have options to decide which SP's operations can be on their VMs and monitor SP's intervention through system log. Therefore, the FCMS helps cloud computing system solve the imbalance of rights between customers and SP.

V. CONCLUSIONS AND FUTURE WORK

From the evaluations of the importance of the balance of rights, this paper proposed a solution to solve the imbalance between the SP and his customers in cloud computing system. The FCMS allows the customer to reject dangerous operations that can cause damage to his VMs. Thus, it helps administration and troubleshooting incidents related to VM contract enforcement. Furthermore, the FCMS makes management of the cloud system more obvious.

In the future, the solution will be implemented in VMM to solve the imbalance of rights completely on the whole system (from VMM to CMS).

The balance of rights does not only reinforce customer's safety with SP's service, but also increases competitive advantages of SPs as they provide mechanisms for VM's safety to their customers.

REFERENCES

[1]. Citrix, Citrix XenServer 6.2.0 Administrator's Guide, 1.1, September 2013, pp.11-17.

[2]. Citrix, Citrix XenServer ®6.2.0 Software Development Kit, June 2013.

[3]. Microsoft, Virtual Machine Manager 2008 R2 Security Guide, July 2010, page 8.

[4]. VMWare, Managing VMware VirtualCenter Roles and Permissions, 2007, page 4.

[5]. VMWare, vSphere Security Guide – ESXi 5.0 – vCenter Server 5.0, 2013, 1, pp.50-59.

[6]. Cao Thanh Phuong, Dang Thanh Phuc, Mai Xuan Phu, Cao Dang Tan, Research on the privileges of the customer and of the service provider on cloud computing systems and propose a solution for the right balance between both sides, undergraduate thesis, 2013.

[7]. VMpros blog, http://blog.vmpros.nl/2010/07/24/vmware-how-to-revert-root-user-role-from-read-only-to-administrator/, retrieved on October 20, 2013.

[8]. Citrix support forum, http://forums.citrix.com/, retrieved on November 4, 2013.