A NEW VIRTUALIZATION-BASED SECURITY ARCHITECTURE IN A CLOUD COMPUTING ENVIRONMENT

Lena AlMutair
lena.almutair@gmail.com

Soha S. Zaghloul
smekki@ksu.edu.sa

College of Computer and Information Science
King Saud University
Riyadh, KSA

ABSTRACT

Cloud computing finally emerged on the stage of the information technology. Virtualization is the core of cloud computing. Virtualization minimizes capital, operational and maintenance costs. Also, it provides flexibility in the used platform. However, the expansion of cloud computing is impeded by the lack of the security issue. Physical resources are exposed to security threats and malware attacks. Therefore, the system is subject to data loss, denial of service, performance degradation, and even hardware damage. This paper proposes a new security architecture based on two frameworks described in the literature. Therefore, the paper explores both frameworks, analyzes them, criticizes them, and then highlights their advantages and disadvantages. Finally, the paper describes the proposed architecture.

KEYWORDS

Cloud Computing; Virtualization; Hypervisor; VMM, Security.

1. INTRODUCTION

Cloud computing is a very promising computing paradigm which recently has attracted both academia and industry. Cloud computing is defined as a pool of virtualized computer resources, it allows to run an application and access data anywhere in anytime, without installing, configuring or maintaining any physical device, it targets a range spectrum of users from individuals to enterprise companies.

Virtualization is a term that refers to the abstraction of computer resources**,** it acts as the fuel for cloud computing**.** Virtualization became recently a necessary component in cloud computing, due to the fact that it is a technology that helps specialized organizations to utilize their application performance in a cost-effective manner. Most of the current interest in virtualization revolves around virtual servers in part because virtualizing servers can result in significant cost savings.

About 70% of users think that data security could impede *cloud computing* fast growth [1]. Users do not feel comfortable allowing cloud commercial provider manage their data servers. In addition, administration and operation are *not* controlled by the user. Also, users question whether physical data are isolated from their rivals. Moreover, the nature of cloud nodes is more vulnerable to attacks than usual solutions, given the hugeness of cloud and underlying service-related complexity that leads to an unprecedented exposure to third parties of services and interfaces. Cloud technology is built on virtualization technology which has limited security capabilities in order to secure a wide area environment such as the cloud. Our motivation is to encourage single users to enterprise companies to use this promising technology, and in return we will make sure that security infrastructure stay at high levels, by discussing several security architectures.

This paper show different architectures for securing cloud computing based on previous studies, it also clarifies the pros and cons of each architecture, how are they different, and when it's considered the best fit for a cloud vendor in a particular environment. This study eases the mission for security architect for developing better security architecture.

This paper discusses cloud computing, the virtualization, and the importance of virtualization in cloud computing. It also discusses the main security threats and attacks. Then, it shows two main security frameworks, and discusses the

advantages and disadvantages of each one and how they are different. The paper concludes by suggesting a framework to cloud vendors; its implementation depends on the environment. A critique of both frameworks is also presented.

The paper is structured as follows: Section 2 reviews the basic concepts of cloud computing and virtualization. Section 3 exposes some related work in this context. Section 4 presents the frameworks under study. Section 5 analyzes the frameworks by highlighting their advantages, disadvantages, and the differences between them. Section 6 discusses the proposed architecture. Finally, Section 7 concludes the paper and sheds light on future work.

2. LITERATURE REVIEW

This study is concerned with two important concepts: cloud computing and virtualization. In addition, security threats are discussed in this section.

2.1 Cloud Computing

Nowadays we are witnessing the emergence of a different technology that enhances business and personal use, the most important one especially from enterprise company perspective is cloud computing. *Cloud computing* is a service model for IT provisioning, often based on virtualization and distributed computing technologies [2]. As commercial activities on the Internet, we already see huge clouds such as Amazon EC2/S3 [3], Google Apps [4], and Force.com [5] by the Internet application vendors.

Cloud is discussed in terms of services: three service models are available at different layers; they are known as *-as-a- Service or *aaS layers:

- Software-as-a-Service (SaaS): access is provided to the software deployed over the internet. This is a "pay-as-you go" model. It was widely initiated for sales force automation and Customer Relationship Management (CRM) [2].
- Platform-as-a-Service (PaaS): a development environment is provided to customers. This service layer provides virtualized servers, OS, and applications [6].
- Infrastructure-as-a-Service (IaaS): a virtualized platform environment is delivered to customers. Rather than purchasing servers, software, data center space and/or network equipment, clients instead buy those resources as a fully outsourced service [6].

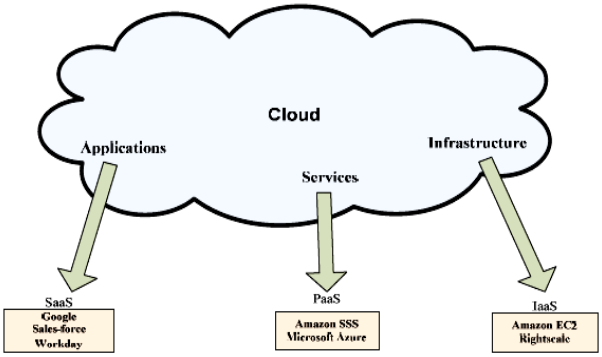


Figure 1. Cloud Basic Services

Iaas is considered the bottom-most layer; it provides the basic infrastructure components such as CPUs, memory, and storage. On the other hand, Software as-a-Service (SaaS) is considered as the top-most layer; it provides users with ready-to-use applications [8].

Figure 2 [9] shows the results of a conducted survey. It shows that about half of all respondents acknowledge that SaaS, IaaS and PaaS resources are not evaluated for security prior to deployment within their organizations.

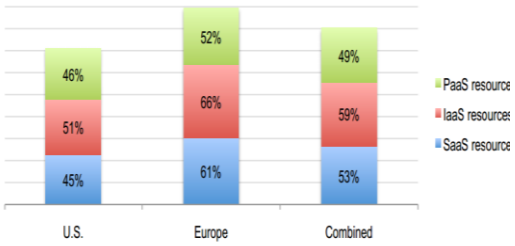


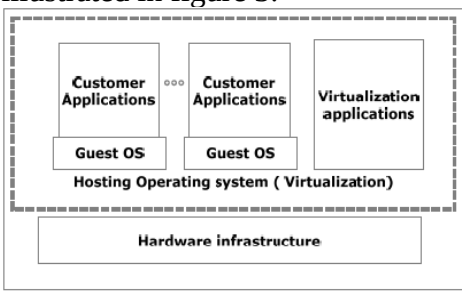
Figure 2 Are cloud computing resources evaluated for security prior to deployment?

2.2 Virtualization

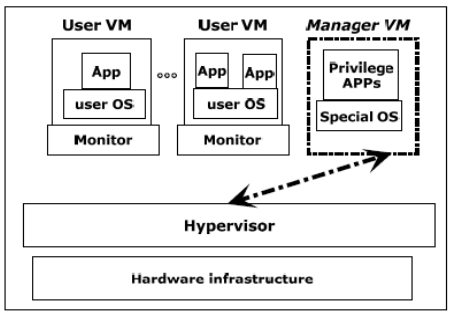
A hypervisor, or virtual machine monitor (VMM), is a core program used in virtualization technology. It allows operating systems to run concurrently on a single host: a feature called hardware virtualization. A *Virtual machine* is an emulated computer that, like a physical computer, runs an operating system and applications. The hypervisor creates and controls all virtual machines installed on the physical machine. Multiple instances of a variety of operating systems may share the virtualized hardware resources.

2.3 Types of Virtualization

There are several virtualization approaches implemented in industry; they differ in the way they manage the virtual machines. These are illustrated in figure 3.



(a) Operating system-based Virtualization



(b) Hypervisor-based Virtualization

Figure 3. Virtualization approaches

2.3.1 Operating System-Based Virtualization

In this approach (Figure 3.a), virtualization is enabled by a host operating system that supports multiple isolated and virtualized guest OS's on a single physical server [10].

2.3.2 Hypervisor-Based Virtualization

The hypervisor is available at the boot time of the physical machine in order to control the sharing of system resources across multiple VMs (see Figure 3.b). Some of these VMs are privileged partitions which manage the virtualization platform and hosted Virtual Machines. In this architecture, the privileged partitions view and control the Virtual Machines. This approach establishes the most controllable environment and can utilize additional security tools such as intrusion detection systems [11]. However, it is vulnerable because the hypervisor has a single point of failure. If the hypervisor crashes or the attacker gains control over it, then all VMs are under the attacker's control. However, taking control over the hypervisor from the virtual machine level is difficult, though not impossible. According to this characteristic, this layer is chosen to implement the proposed security architecture [10].

2.4 Cloud and Virtualization Security Issues and Threats

Cloud - One of the key issues of cloud computing is loss of control. For example, the service user (SU) does not know where exactly its data is stored and processed in the cloud. Computation and data are mobile and can be migrated to systems the SU cannot directly control. Over the Internet, data is free to cross international borders and this can expose the user to further security threats. Another example of loss of control is that the cloud provider (CP) gets paid for running a service he does not know the details of. This is the dark side of the ''Infrastructure as a Service''.

Some of the security issues of a cloud are [12]:

- Privileged user access
- Data segregation
- Privacy
- Bug Exploitation
- Recovery
- Accountability: even though cloud services are difficult to trace for accountability purposes, in some cases this is a mandatory application requirement.

Virtualization Threats - It can increase the security of cloud computing, by protecting both the integrity of guest virtual machines and the cloud infrastructure components [2].

With the hypervisor, all users see their systems as self-contained computers isolated from other users, even though every user is served by the same machine. In this context, a Virtual Machine is an operating system that is managed by an underlying control program.

Virtual machine level attacks: the hypervisor and/or virtual machines used by cloud vendors are a potential problem in multi-tenant architecture [13].

Cloud provider vulnerabilities: These could be platform-level, such as an SQL-injection or cross-site scripting vulnerability that exist in cloud service layer which cause insecure environment.

Expanded network attack surface: The cloud user must protect the infrastructure used to connect him with the cloud; this task is complicated by the cloud if the firewall is abandoned: a scenario found in many cases [13].

***Authentication and Authorization*:** The enterprise authentication and authorization framework does not naturally extend into the cloud. Enterprises have to merge cloud security policies with their own security metrics and policies.

Lock-in: The cloud provider can encrypt user data in a particular format. If the user decides to migrate to another vendor with an incompatible format, this will impose a problem on the user [14].

***Data control in cloud*:** Midsize businesses are used to have complete visibility and control over their entire IT portfolio. However, moving some components into the cloud creates operational "blind spots", with little advance warning of degraded or interrupted service [15].

Communication in virtualization level: Virtual machines have to communicate with each other. In some cases, they may need to share data. If these communications didn't meet significant security parameters, then they are subject to attacks.

Virtualization Attacks - Basically, as the cloud gives services to legal users, it can also services to users that have malicious purposes. A hacker can use a cloud to host a malicious application to achieve his object which may be a DDoS attacks against the cloud itself, or targeting another user in the cloud. For example, an attacker knew that his victim is using a cloud vendor with name X, now attacker by using similar cloud provider can sketch an attack against his victim(s). This situation is similar to this scenario that both attacker and victim are in the same network, but with the difference that they use virtual machines instead of physical network (Figure 4) [14].

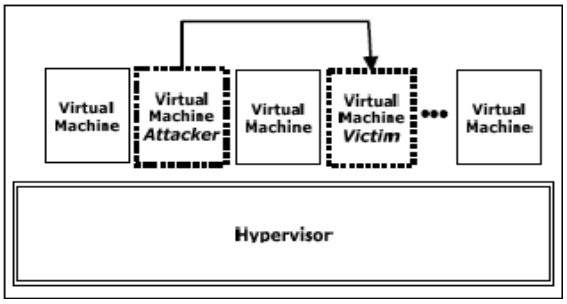


Figure 4. Attack scenario within cloud

Attack between VMs or between VMs and VMM: One of the primary benefits that virtualization brings is isolation. This benefit, if not carefully deployed becomes a threat to the environment. Poor isolation or inappropriate access control policy causes the inter-attack between VMs (virtual machine) or between VMs and VMM (virtual machine monitor) [1].

Client to client attacks: One malicious virtual machine could infect all virtual machines installed on the same physical server. This is the biggest security risk in a virtualized environment [10].

Virtual machine controlled by Host Machine: The host monitors all the network traffic going to/ coming from the VMs through the host. Therefore, if a host is attacked, then the security of the VMs is under question. Hence precautions should be taken while configuring the VM environment in such a way to provide enough isolation; this avoids the host being a gateway for attacking the virtual machine [1].

Denial of Service: A denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a computer resource unavailable to its intended users. In virtual machine architecture, the guest machines and the underlying host share the physical resources such as CPU, memory, hard disk, and network resource. So it is possible for a guest to impose a denial of service attack to other guests residing in the same system. Denial of service attack in a virtual environment can be described as an attack when a guest machine takes all the possible resources of the system [1].

VM sprawl: VM sprawling is a case in which the number of VMs is continuously growing, while most of them are idle or never back from sleep. This causes a large waste of the host machine's resources [1].

3. RELATED WORK

Many studies were dedicated to provide a secure virtualized environment in cloud computing. Here are some of them:

- In [2], the authors proposed a security architecture to protect the cloud based. The idea is based on virtualization; it is called Advanced Cloud Protection System (ACPS). It consists of a monitor key kernel or middleware component that is able to

detect any modification to the kernel data and code. It also checks the behavior and the integrity of cloud components via logging and periodic checksum verification of executable files and libraries to manage monitoring cloud entry points. The system is implemented using open source code OpenECP and Eucalyptus.

- In [16] discussed a problem that current cloud computing services suffer from. More explicitly, this is the inability of isolating the computing resources and network between customers. This implies that data packets may share the same LAN. Such lack of isolation brings security risks to the users. Moreover, the scalability limitations of prior VLANs-based solutions do not allow the users to customize security policy settings the same way they control their on-site network. Therefore, an architecture that uses network virtualization as the main component for the security is suggested.
- [17] shows that it is possible to instantiate an increasing number of guest VMs until one is placed co-resident with the target VM. Once successfully achieved, attacks theoretically extract information from a target VM on the same machine. An attacker might also actively trigger new victim instances exploiting cloud auto-scaling systems. The author proves that co-residence is practical and simple.

4. VIRTUALIZATION SECURITY FRAMEWORKS ANALYSIS

In this section, common virtualization-based frameworks are discussed.

4.1 First Framework

The first framework [1] is organized effectively in two modules which are:

- virtual system security
- virtualization security management

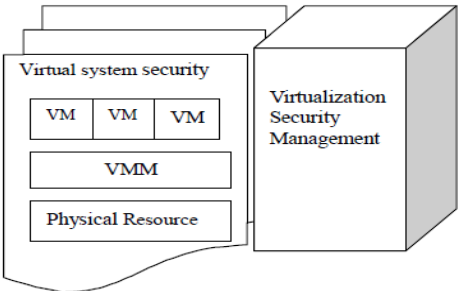


Figure 5. Virtualization Security of Framework 1

Figure 5 illustrates the first framework: two modules perform their duties without disturbing each other, so that the entire framework can be more efficient.

The virtual system security consists of three layers:

- The first layer is the Physical Resource layer.
- The second layer is VMM which is the most important layer: this should be provided with security mechanisms that the VMs while running.
- The top layer is that of the VMs that provide virtualization services to consumers. Virtualization security management protects the framework from attacks and threats.

Virtual System Security

This consists of four parts:

- The VM system architecture security.
- The access control framework.
- The virtual firewall.
- The Virtual Intrusion Detection System (VIDS) / or Virtual Intrusion Prevention System (vIPS)

VM system architecture security

A secure VM system should be protected by a robust, efficient and flexible VM system architecture. The system architecture is illustrated in Figure 6. The structure spares some of the VMM administration task to a special VM, called admin VM. This cooperates with the VMM to manage the other VMs.

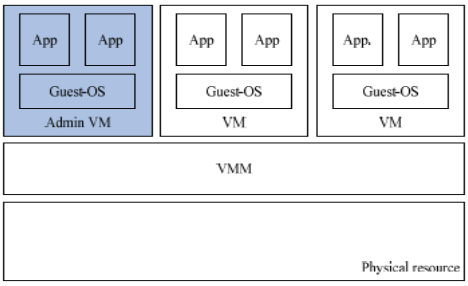


Figure 6. VM system architecture where admin VM is deployed in the VM

Access control
It refers to the practice of restricting entrance to a resource to authorized VM. An access control framework for virtual system is shown as Figure 7.

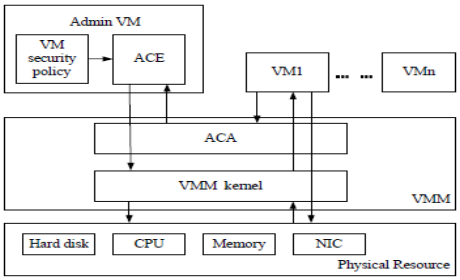


Figure 7. An access control framework

An access control framework is divided into three layers, namely:

- Physical resource layer
- Virtual machine monitor system layer
- Virtual machine system layer.

As shown in Figure 7, the physical resource layer contains the required hardware resources of the entire structure. This access control framework mainly consists of Access Control Agent (ACA) residing in VMM and Access Control Enforcer (ACE). In turn, this resides in the Admin VM which is in charge of managing the whole virtual system cooperating with VMM. ACE is used to control guest-VM access behaviors as per its security policy profile. ACA is used to receive the requests from guest-VM, and then transfer them to the ACE. In the access control structure, Admin VM plays an important role as an agent. The VMM system delivers the work of the security policy profile to the Admin VM, and then VMM system controls the guest-VM according to the requirements of the Admin VM. Adding an Admin VM in the access control framework provides the whole structure with simplicity and flexibility.

Virtual firewall
A Virtual Firewall (VF) is a firewall deployed entirely within a virtual environment. It provides packet filtering and monitoring. A virtual firewall protects the network and computers from outside threats, including hackers and malicious attacks.

Virtual Intrusion Detection & Prevention System
Nowadays, there is a variety of attacks in the network. The extent to which a system can effectively resist the network attacks is a measure of the system security. vIDS/vIPS protects virtual environment by collecting and analyzing information from network and host to check if there are any signs of attacks.

Virtualization Security Management
The virtual machine security management is divided into four parts: patch management, VM migration management, VM image management, and audit.

Patch management is an area of systems management that involves acquiring, testing, and installing multiple patches (code changes) to an administered computer system.

VM migration management VM migration is a vulnerable process that is easily attacked. When a VM is going to migrate to somewhere, particular security mechanisms should be taken into account. The security and compliance postures of physical servers must be analyzed to ensure that sensitive workloads are not collocated in ways that create security or compliance risks.

VM image management (VMI) is a special type of file/data format which is used to instantiate (create) a virtual machine within the virtual environment. So the confidentiality and integrity of VMI is of great importance when VM is under bootstrapping or migrating.

Audit VM behaviors and sensitive data should be monitored during its lifecycle. Auditing may provide a mechanism to log all the trace of the activities left by the virtual system. When the destruction of the virtual system or the sensitive data occurs, we can diagnose the reasons of destructions of the system and/or data quickly through these records. Then, based on these records, we can develop the appropriate strategies against these future harmful behaviors [1].

4.2 Second Framework

Some features are added to the virtualization architecture in order to improve security for cloud environment. In addition two main units of proposed architecture [10] are based on this truth:

"When the workload of the VM increases abnormally, the VM may be a victim or an attacker" [10]

Therefore, the architecture included additional units to monitor the events and activities of the VMs, while trying to prevent attacks without knowing what type of data is being transmitted between VMs or VMs and hypervisor.

Framework 2 has added some new features to increase security performance in virtualization technology such as security and reliability monitoring units (VSEM and VREM). HSEM and HREM are the main components of the security system, and all the other parts of the security system communicate with them, but HSEM decides if the VM is an attacker or a victim. Actually, HSEM receives behavioral information from VSEM and HREM and never collects any information itself. In addition, HSEM notifies the hypervisor about which VM is under Level-2 monitoring in order to set service limits until the status is determined. Figure 8 illustrates the architecture and the additional units in VMs level, VSEM and VREM. These are made available for all VMs. In addition, there are two other units, HSEM and HREM, which are made available at the hypervisor level. VSEM and VREM consume low resources of the VM, but they help to secure VMs against attacks.

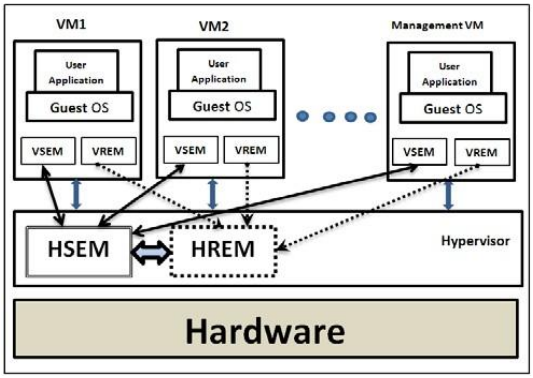


Figure 8. Architecture of secured virtualization

VM Security Monitor (VSEM)

There is a VSEM within every VM that is running in a virtual environment. VSEM is a two-level controller and behavior recorder in the cloud system that helps HSEM identify attacks and malicious behavior with less processing. VSEM monitors the security-related behaviors of VMs and reports them to HSEM. Because there is a large number of transmissions in the cloud, sending all of them to HSEM consumes a lot of bandwidth and processing resources, which can affect the general hypervisor activity. Therefore, some tasks are done by VSEMs in VMs such as collecting information. In addition, because users don't want to consume their resources, which they paid for, VSEMs have two levels of monitoring that consume more resources only when it is necessary. Actually, each level of VSEM is monitoring almost the same events but at different detail levels.

Level 1- In this level, the VSEMs monitor their own VMs. In this level VSEM collects of the source and destination addresses which are in head of data, number of unsuccessful and successful tries in sending data, and number of requests that were sent to the hypervisor. At this level, VSEM, according to the brief history of the VM which provided by HSEM, looks for anomaly behavior (HSEM has had history of VMs in more details). For instance, the system identifies the VM as a potential attacker or victim if the number of service requests from the hypervisor is higher than average based on the history of requests of the VM. If abnormal behavior is detected, or the type of sending data and unsuccessful tries increase above that threshold (according to history of the VM), then VSEM switches to Level 2 and also notifies HSEM about this switching in order to HSEM investigates the VM for finding malicious activities.

Level 2- In this level, the VSEM monitors and captures the activity of the VM in more detail, such as VM's special request from the hypervisor, details of requested resources (e.g. the number of requests), and the destination transmitted packets (to recognize if it is in the same provider's environment or outside). In this mode VSEM notifies HSEM about the level of monitoring in the VM. According to this notification, the hypervisor set activity limits in types of activities until HSEM learns that the VM is not an attacker or victim. At this level, HSEM makes a request from VREM about the reliability status of the VM, including the workload status and how many times the VM

workload was close to the maximum capacity of the VM.

VM Reliability Monitor (VREM)

VREM monitors reliability-related parameters, such as workload, and notifies the load-balancer (within the hypervisor) about the parameter results. VREM is also used for security purposes. The VREM will send useful information such as workload status to HREM and requests the status of the VM from HSEM, and then it decides whether to give the VM more resources. Actually, if the VM requests as many resources as it can (that is different behavior according to its usage history), it may signify an overflow attack victim. Therefore, proposed HREM can detect overflow attacks and notify the HSEM about it.

5. ANALYSIS OF FRAMEWORKS

In this section, the previously explained frameworks are analyzed.

Pros of Framework 1

- Have two modules which are virtual system security and virtualization security management. Each one of them has its own functionality and performs their duties without disturbing each other, so that the entire framework can be more efficient.
- Virtual system security module restricts the resource to allow only authorized VM.
- Virtual system security divided to three parts, each one of them specialize in a security issue, it applies the decomposition, which is a good approach in designing a new architecture
    - *Access control* gives the authorization and limitation for a VM to use the resources upon to the VM's security profile.
    - *Virtual firewall* running entirely within a virtual environment and which provides packet filtering and monitoring, so it protect the network and nodes connected to it from outside threats.
    - *Virtual Intrusion Detection & Prevention System* its turn to resist the network attacks by collecting and analyzing information from network and Host to check if there are signs of attacking.
- Detection and prevention mechanism is applied in this framework via *vIDS/vIPS.*
- The management and security work is divided between VMM and admin VM, so the overhead in VMM reduced.
- The other module of the system is *virtualization security management* it takes care of patch management, VM migration management, VM image management, and audit. Each one of them put corresponding measure for the problems which may be present in the event of the virtualization security management.

Cons of Framework 1

- It cause overhead in case of huge number of VM connected to one physical server.
- Response and performance degraded as new VM get bound to the current physical server.

Pros of Framework 2

- Virtual machine security management VSEM component have two levels of control and a behavioral recorder; these records help the HSEM to infer the status of VM.
- In order save resources usage that user paid for, framework define two levels in VSEM, so it consume more recourses only when it's needed (i.e. when VM detected with suspected behavior VSEM will switch to level 2)
- Framework is flexible and dynamic; when VSEM switch to Level 2, it informs HSEM about it, to limit the resources for that VM until it learns that VM is neither attacker nor victim.
- Detection and prevention mechanism is applied in this framework.
- The existence of reliability component VREM which monitor the reliability of the VM (i.e. workload).
- VREM is smart, it sends workload status to hypervisor reliability management (HREM), then, in its turn to request the status of the current VM from HSEM (since it keeps record history of VMs), so it can decide whether to allow VM to use more resources.

Cons of Framework 2

- Security component VSEM and VREM will consume resources, which user paid for.
- Can't define whether the suspected VM victim or attacker.

Comparing both frameworks, we find that framework 1 consumes a high bandwidth; because when VM want to access the recourses, it consults ACA component in VMM which in its turn consult ACE component in Admin VM, which involve a high rate of bandwidth wastage, unlike framework 2, it divides the security task between hypervisor and VMs via distributing the security component over hypervisor and all VMs, so there is a component in VM gather behavioral information then send it to a component in hypervisor which in its turn takes the decision. in addition, Framework 2 virtual machine manger analyze the need for all new Virtual Machines carefully and ensure that any unnecessary Virtual Machines migrate to other physical servers, meanwhile, Framework 1, doesn't do any smart migration when VM created (doesn't take the decision by its own).

6. PROPOSED ARCHITECTURE

We already have shown some of good framework, and discuss the pros and cons of each system, now with taking care of these advantages and with some trade of, we propose two solutions.

6.1 Solution 1

In this framework **Figure 9**, it resolves some of the problem of both frame work by reducing the overhead on VMM, since VMC (Virtual machine control) analyzes VM behavior then, it provides the VMM with the behavioral report.

Whenever the VM acquires resources, VMC informs about the behavioral report with the request.

ACA is used to receive the requests from guest-VM, and then transfer them to the ACE**,** and ACE is used to control guest-VM access behaviors as per its security policy profile.

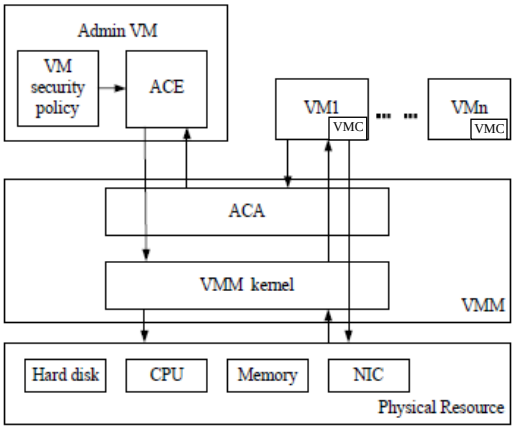


Figure 9. Virtual machine control

Admin VM plays an important role as an agent. The VMM system delivers the work of the security policy profile to the Admin VM, and then VMM system controls the guest-VM according to the requirements of the Admin VM and received information from VMC. So, if there's any threat, VMC sends the recorded behavioral activity. These are measured according to ratio of the number of the usual activities to the number of the current activities recorded by the VMC component. Consequently, the VMM limits the resources for this suspected guest-VM.

The solution is considered effective for different reasons. First, the addition of an Admin VM in the access control framework provides the whole structure with simplicity and flexibility. Unlike framework 1, where the VM consumes a great amount of bandwidth by frequently consulting the VMM, this issue is overcome in the proposed solution by introducing the VMC component. The latter is considered a key parameter to the VMM decision. On the other hand, in framework 2, users pay a great deal of money for the resources that are actually used by the security system component since it involves two components that reside in each VM.

Therefore, the proposed solution is derived by combining the advantages of pre-discussed frameworks. In addition, the disadvantages in the new framework are minimized. The proposed framework manages to minimize the bandwidth wastage between VMs and VMM. In addition, it reduces the costs of the security resources for the users, by minimizing the component of security framework in an effective way.

6.2 Solution 2

The other solution proposes to add a security layer whose role is to resolve security and performance issues. The VMM layer is therefore thinner because it is only concerned with management tasks. This is illustrated in Figure 10.

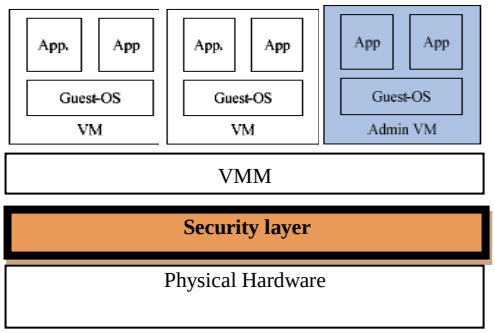


Figure 10. Framework Architecture with Security Layer

This framework achieves the highest efficiency and flexibility. In addition, it is considered the safest in the security system, since it uses the layers approach; each layer is assigned with predefined functionalities. However, it is considered more complex than the other architectures: the security control is separated from the VMM layer. In addition, security control for the VMM layer is transparent. While the VMM layer focuses on the VM management tasks, VMs are protected by both the security control layer and admin VM**.** As a result, the VMM becomes thinner and delegates all security tasks to the security control layer which will run even before VMM.

7. CONCLUSION AND FUTURE WORK

This study focuses on some security issues that impede cloud fast growth. It then explores two security frameworks that are exposed in the literature. This paper highlights both the advantages and the disadvantages of each framework. In addition, a comparative study is conducted between both frameworks. This analytical study leads us to two solutions.

The first analyzed framework is used efficiently whenever there are a reasonable number of virtual machines. This is because all VMs are bounded to a single VMM. Therefore, the consumption of a huge bandwidth between the VMs and the underlying VMM is considered a burden.

On the other hand, if there is a big number of VMs, then the second framework is a more suitable solution. From the user's perspective, this framework consumes expensive resources for the sake of security provision. However, from the CSP's perspective, the security management is decentralized. Therefore, the bandwidth consumption between the VMM and the VMs is reduced.

The first solution proposed in this paper is suitable in case there is a big number of VMs. This is explained by the existence of the decentralized security component. Therefore, the bandwidth consumption between the hypervisor and the VMs is reduced.

On the other hand, the second solution proposed in this paper follows a modular approach in which the VMM is concerned with the management of VMs, and the security layer takes care of security issues.

In the future work, these two proposed solutions are to be simulated. The performance of both of them is to be evaluated and reported.

8. REFERENCES

[1] Luo, S., Lin, Z., Chen, X., Yang, Z., Chen, J.: Virtualization security for cloud computing service. In IEEE International Conference for Cloud and Service Computing (CSC), (2011).

[2] Lombardi, F., Di Pietro, R.: Secure virtualization for cloud computing. Journal of Network and ComputerApplications, 34(4), (2011).

[3] Amazon: AmazonWebServices, http://aws.amazon.com/

[4] Google, GoogleApps, http://www.google.com/apps/intl/en/business/index.html

[5] Salesforce.com, Force.com, http://www.salesforce.com/platform/

[6] Yang, J., Chen, Z.: Cloud computing Research and security issues. In IEEE International Conference on Computational Intelligence and Software Engineering (CiSE), (2010).

[7] Bhadauria, R., Chaki, R., Chaki, N., Sanyal, S.: A Survey on Security Issues in Cloud Computing. arXiv:1109.5388, (2011).

[8] Jensen, M., Schwenk, J., Gruschka, N., Iacono, L.: On technical security issues in cloud computing. In IEEE International Conference on Cloud Computing (CLOUD'09), (2009).

[9] Ponemon, L.: Security of Cloud Computing Users: A Study of Practitioners in the US & Europe. Ponemon Institute Research Report, (2010).

[10] Sabahi, F.: Secure Virtualization for Cloud Environment Using Hypervisor-based Technology. Int. Journal of Machine Learning and Computing, 2(1), (2012).

[11] Litty, L. Hypervisor-based Intrusion Detection. Doctoral dissertation, University of Toronto, (2005).

[12] Foster, I., Zhao, Y., Raicu, I., Lu, S.: Cloud Computing and Grid Computing 360-degree Compared. In Grid Computing Environments Workshop, GCE'08, (2008).

[13] Chow, R., Golle, P., Jakobsson, M., Shi, E., Staddon, J., Masuoka, R., Molina, J.: Controlling Data in the Cloud: Outsourcing Computation Without Outsourcing Control. In Proceedings of the 2009 ACM workshop on Cloud Computing Security, (2009).

[14] Sefton, P.: Privacy and Data Control in the Era of Cloud Computing. Brightline Lawyers, (2010).

[15] Rowe, D.: The Impact of Cloud on Mid-size Businesses. [Online]. Available: http://www.macquarietelecom.com/hosting/blog/cloud-computing/im, (2011).

[16] Hao, F., Lakshman, T., Mukherjee, S., Song, H.: Secure Cloud Computing with a Virtualized Network Infrastructure. In Proceedings of the 2nd USENIX Conference on Hot Topics in Cloud Computing (HotCloud'10), (2010).

[17] Ristenpart T, Tromert E, Shacham H, Savage S.: Hey, You, Get Off of my Cloud: Exploring Information Leakage in Third-party Compute Clouds. In Proceedings of the 16th ACM Conference on Computer and Communications Security, (2009).