International Journal of Security and Its Applications
Vol. 11, No. 5 (2017), pp.49-58
http://dx.doi.org/10.14257/ijsia.2017.11.5.05

An Algorithm to Secure Virtual Machine Image in Cloud Environment

Preeti Thakur[1] and Devesh Kumar Srivastava[2]

[1]Computer Science & Engineering Department,Manipal University, Jaipur,Rajasthan, India
[2]Computer Science & Engineering Department,Manipal University, Jaipur, Rajasthan, India
[1]preeti_thakur3@yahoo.com, [2]devesh988@yahoo.com

Abstract

Virtual Machine is a combined form of operating system and application. Virtualization provides the facility to run multiple operating systems on a single physical machine. These multiple operating systems are called guest operating systems. In server Virtualization many virtual machines (VMs) can run on one server including its own server. These VMs can be migrated from one server to another. As VM image will be downloaded to create a new virtual machine on the guest operating system it has some security problems. Unauthorized access can create the security issues like Malware injection. Due to which there is a need of scheme capable of providing encryption, malware detection, automatic patching to restore the image. In this paper an algorithm is proposed which is capable of providing solution to the above issues.

Keywords*: Virtual Machine, Virtual Machine Image, VM Migration, Securitycloud*

1. Introduction

Cloud computing is used to share the configurable computing resources which are on demand to a shared pool of network. NIST define the cloud "Cloud computing is a model that enables on demand,scalable network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal effort of management or service providers interaction". There are various types of services provided by the cloud computing environment. Some of them are listed below:

1.1. Service Model of Cloud Computing

Infrastructure-as-a-service (IaaS)

In this type of service the consumer is provided fundamental computing resources. The consumer can run their software using those fundamental resources. The consumer does not require the management or control the underlying cloud infrastructure but has control over operating system, storage, deployed applications, and possibly limited control of select networking components (*e.g.*, host firewalls). Infrastructure as a service is provided by several servise provider like Amazon,Microsoft.Since the IaaS cloud delivery model eliminates the need to invest in hardware,it s perfact solution for startups and for organizations that deal with extreme spikes and troughs in usage.In recent timings the distinguishing line between the IaaS and PaaS services is diminishing as cloud service providers move towards rendering deployment tools as a part of their IaaS offering.

ISSN: 1738-9976 IJSIA

Platform-as- a-Service (PaaS)

PaaS provides the environment in which the application will be developed. With PaaS application can be created and modified. It provides the platform to SaaS application delivery model. PaaS is the best fit for organization that are commited to the delivery of web and mobile application within a stipulated time and budget. A Paas provider offers the toolkit to build an application and the virtual machine to run it.for example IBM BlueMix,Google App Engine etc. Applicationusing PaaS possess the ability to inherit all characterstics of the cloud like multitenency, scalibility,SaaS enablement.

Software-as-a-Service (SaaS)

In this type of service the customer is having no control over the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities. The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure.

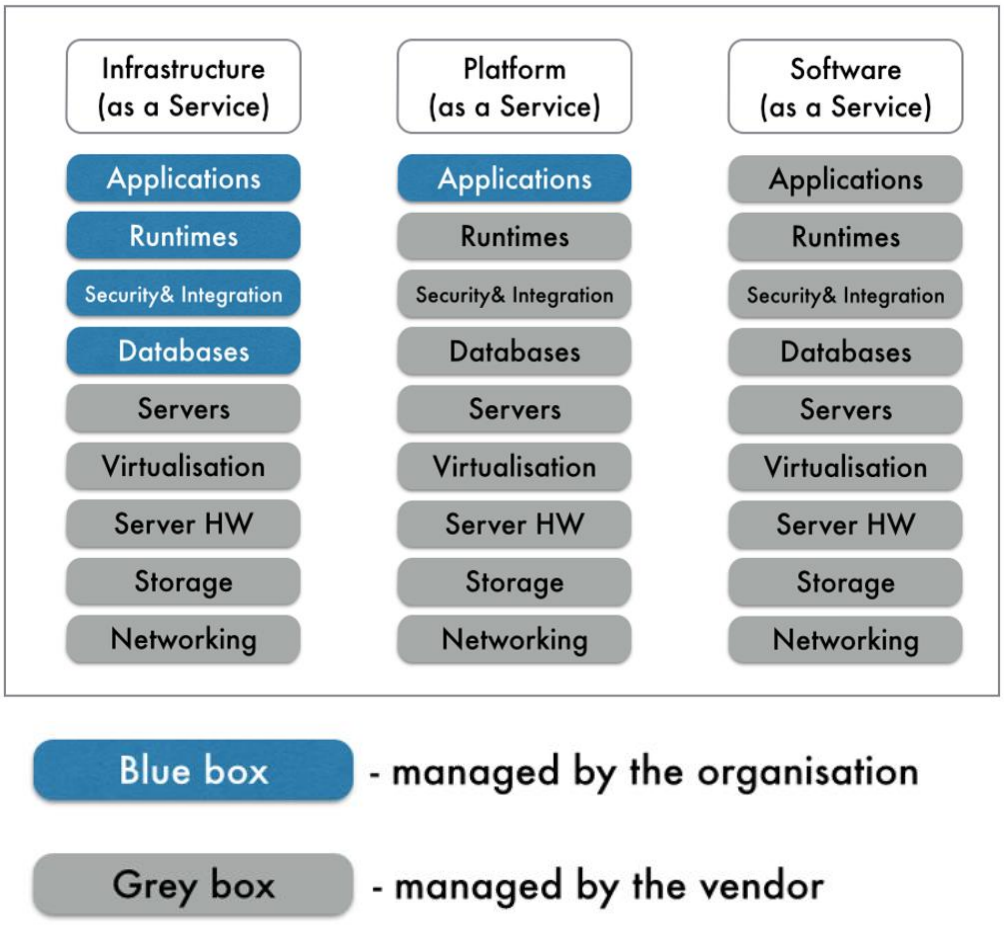

Figure 1. Cloud Computing-Difference between SaaS, PaaS and IaaS

1.2. VM Image

VM Images are necessary to create VMs. These Images are fundamental of security in VM Migration [1-2]. Attacker can store Images having malicious code into public repository, compromising cloud and other users [4-6]. While an Image is being created, some confidential information may be recorded. These kind of Images need to be cleaned, otherwise sensitive information will be exposed in public.

1.3. Virtualization

In computing, virtualization means to create a virtual version of a device or resource like storage, server, network or even an operating system where the framework divides the resource into one or more execution environments. Virtualization technique is associated with a number of computing technologies including the following:

Storage Virtualization

Storage Virtualization is the process of dividing the physical storage into several virtual storages to the Virtual machines. These virtual machines are called guest machines.

Server Virtualization

It is the process of dividing the physical server into several virtual servers

Network Virtualization

It is the process of dividing the total network resources into several smaller logical network resources (Virtual network).

1.4 Virtual Machine and its Security Challenges

A virtual machine image is a single file which contains a virtual disk having installation file of bootable operating system. Virtual machines are becoming more common because of virtualization technology. Virtual machines are created to perform certain tasks that are different than tasks performed in a host environment. Architecture of Virtual machine is depicted in figure 2.

During Live VM migration, configuration files and memory images are sent from one server to another. These files and memory images are in combined form called VM Images. If these images are not protected attacker can make changes in the images or may steal any private information from the Images.

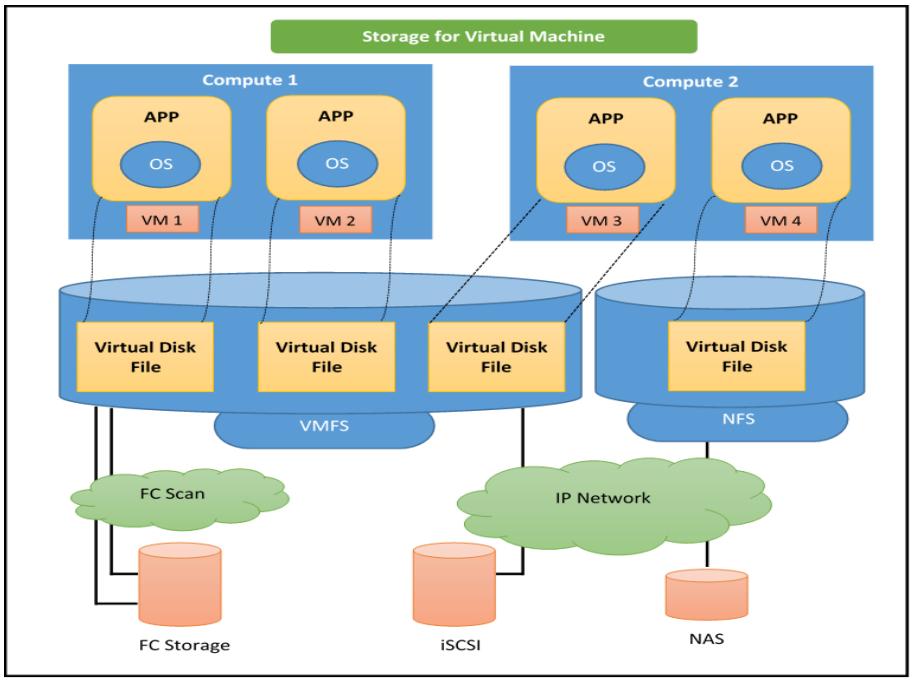

Figure 2. Architecture of Virtual Machine storage

System Virtual Machines

System virtual machine is a platform to share the host computer's physical resources among multiple virtual machines. A separate copy of the operating system is running on each system. There is a software layer called hypervisor to support the virtualization technique. Two types of hypervisors are available one can run on bare hardware another type runs on top of an operating system.

Process Virtual Machine

It provides a platform-independent programming environment. It allows the program to be executed just the same like on any given platform by masking the information of the underlying hardware or operating system.

1.5 Challenges in virtualization

Although virtualization technology has given new technical and economical advancement still this new software layer comes with new security issues. Below is the list of challenges given by Garfinkel and Rosenblum [14] occur due to virtualization.

Scaling

Creating a new physical machine depends on the organization’s capital investment but new virtual machines can be easily created by virtualization just like copying a file in to new file. This also increases the management complexity. The unexpected growth of virtual machine then needed much more security, flexible network policies (setup, updates...). This is a big issue in virtual machines security.

Transience

There is a collection of specialized VMs in virtual environment. So traditional computing environment can be put in to a good or stable state but with so many transient machines it is almost impossible to stabilize the system. In conventional system the administrator can find the malicious machine and patch and network can be back into steady state but It will be difficult to find the particular infected machine and clean them up.

Software Lifecycle

A Virtual Machine can be restored to a previous state but raise many security concerns. One of them is the reappearance of previously patched vulnerabilities. Moreover, an attacker can repeat some sequences obsolete at the time of restoration if restoration process applied on virtual machine.

Diversity

In virtualization there is an increasing risk of having many version of same system at the same time on the network as in many organizations security policies are based on the homogeneity of the machines. Many IT organizations tackle security problems by enforcing homogeneity: all machines must run the most current patched software. VMs can facilitate more efficient usage models which derive benefit from running unpatched or older versions of software. This creates a range of problems as one must try and maintain patches or other protection for a wide range of OSes, and deal with the risk posed by having many unpatched machines on the network. For example, at many sites today users are simply supplied with VMs running their new operating environment and applications are gradually migrated to that environment, or conversely, legacy applications are run in a VM. This can mitigate the need for long and painful upgrade cycles, but leads to a

proliferation of OS versions. This makes patch management more difficult, especially in the presence of older, deprecated versions of operating systems.

Mobility

Like a file stored on the disk, we can copy virtual machine and easily move to another disk or any other host. Although this feature is one of the benefits of virtualization yet it adds security constraints because security can only be guaranteed if every host on which there is a virtual machine be secure.

Identity

Mobility increases the difficulty of the authentication process of virtual machine ownership as it can be copied or moved easily like a file on hard drive. Usual methods used to identify machines (like MAC addresses) are not necessarily efficient with virtual machines.

Remainder of this paper arranged as follows: Section II will discuss the related review of virtual machine image security. Section III will provide the proposed algorithm for authentication Section IV will be the Result and section V will be conclusion and future scope.

2. Related Review

VM Images specify the initial state of the VM, they need high level of security.VM Images are used by various related and unrelated users. For the security of whole cloud computing environment, it is necessary to secure VM Images. This may be achieved by using virtualization aware security tools and also implementing them in cloud computing environment. There are following VM images security mechanisms which are proposed by different researchers.

2.1 Mirage

Mirage [7], structure is shown in figure 3 is an image management system which manages VM image and provides security in four ways.

Access Control

Any user who wants to modify or publish VM Images needs proper permission. Each image in the repository has a unique owner, who can share images with trusted parties by granting access permissions. It support two types of access permissions, checkout and checkin. A checkin permission implies checkout permission. Retrieving and running an image requires checkout permission. Revising an image and storing the revised image in the repository requires checkin permission.

Filters

Filters are used to hide the sensitive information at publish time from original image. There are two types of filters Remove Filter and Hide Filter. Remove filter removes sensitive information from the Image. Hide Filter hide the private information or replaces it in safer version.

Auditing

In auditing all operations performed on images are reviewed from a tracking file. A tracking file is created by recording the derivation history of an image.

Maintenance Services

Maintenance services run detection tools to find vulnerabilities, virus or any license regarding issues. It is not easy to monitor the dormant images as it is a time consuming task. This approach provides the repository services for effective maintenance.

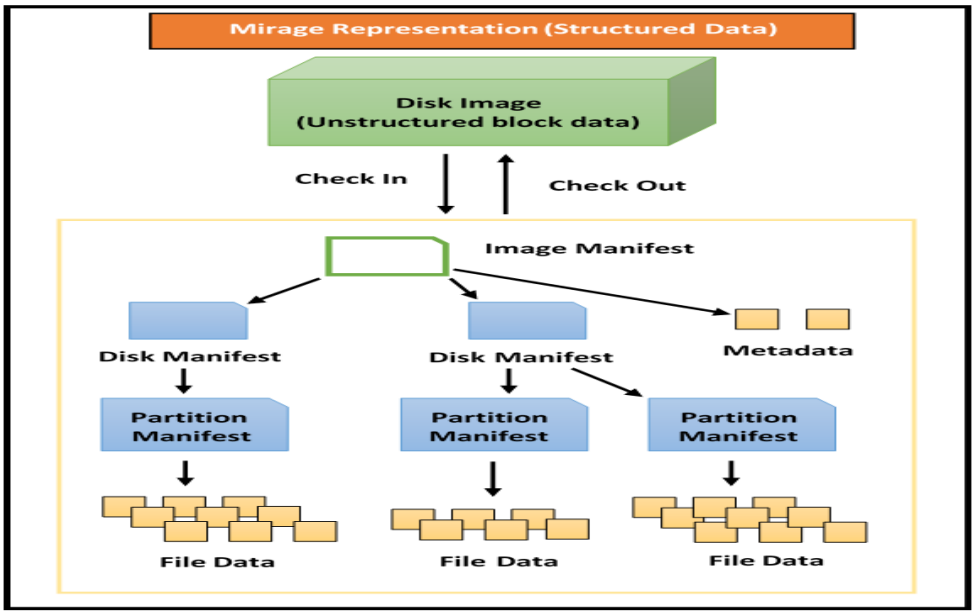

Figure 3. Structure of Mirage

2.2. EVDIC

EVDIC proposed by [8] encrypts the VM Images. EVDIC uses AES of key size 256 bits. There are two modules:

Image Encryption Module:

The images are stored in encrypted form on the disk. In this module an image is encrypted whenever a VM is terminated. The method used to encrypt is AES (advanced encryption module) with 256 bits as key size. The key is generated by a third party called key management server through the proper identification of the user. Then that encrypted image is stored back on the disk.

Image Decryption Module:

Virtual machine is loaded with the help of the key used to decrypt image. This key is generated by key management server and provided to decryption module of EVDIC

EVDIC presents integrity information for the VM images to provide integrity and confidentiality services to the VM images.

2.3 Online Penetration Suite (OPS)

[12] Provides an approach to reduce the vulnerabilities in VMs by patching. Patching is done manually. Two types of modules work in the online penetration suite:

Update Checker

To set up a cloud track of all software being required by the virtual machine are kept as a record in this module like their version number, update and release *etc*. VM is checked

at the time of registration and periodically. For software there is a record that matched against installed and available packages. These records are kept safe in central database.

OPS

It discovers software vulnerabilities from VMs using reputable security practices. Update checker and OPS both give result report to both the system administrator and the user of VM. The goodness of the scheme is that administrators can have a check for outdated software does not run on their system and the user can keep the VMs updated.

2.4. ImageElves

It is another approach proposed in [10]. It provides updated software installs, and patches for the virtual machines in the cloud. ImageElves works similar to the technique presented in [9]. It keeps record of all the software running on the VMs. The ImageElves is useful for both on the running and dormant VM images.

Table 1. Comparative Analysis of Approaches for Virtual Machine Image Security

Scheme	Integrity &Privacy	Access Control	Malware Protection	Outdated Software Detection
Mirage	No	Yes.	**No**	**Yes**
EVDIC	Yes	Yes	Yes(only for dormant images)	No
Online penetration suite (OPS)	No	No	No	Yes
Image Elves	No	No	No	Yes
Offline Patching Scheme	No	No	Yes	Yes

3. Proposed Algorithm to Secure Virtual Machine Image

An algorithm is proposed in this paper for access control so that no unauthenticated person will get authorization to Virtual machine image. In this algorithm the OTP method is used to verify the user.

Step 1: Encryption of the virtual machine image by some Encryption Algorithm like AES, RSA *etc*.
Step 2: Save the Image on host server's image library.
Step 3: To create a new virtual machine instance on guest server the client has to register the MAC address of the machine along with the VM Id on to the cloud database by some interface provided to register.
Step 4: A log table should contain the entries in pair of MAC address and virtual machine Id.
Step 5: Based on the MAC address an OTP will be send to the client machine in every 10 min to authenticate the user.
Step 6: Once the client has been authenticated by checking the details (OTP, VM_ID) from the Authenticate server database he/she can create a new virtual machine.

Step 7: Every time whenever the host server accessed the same process of authentication will perform

The above process is shown below in Figure 4.

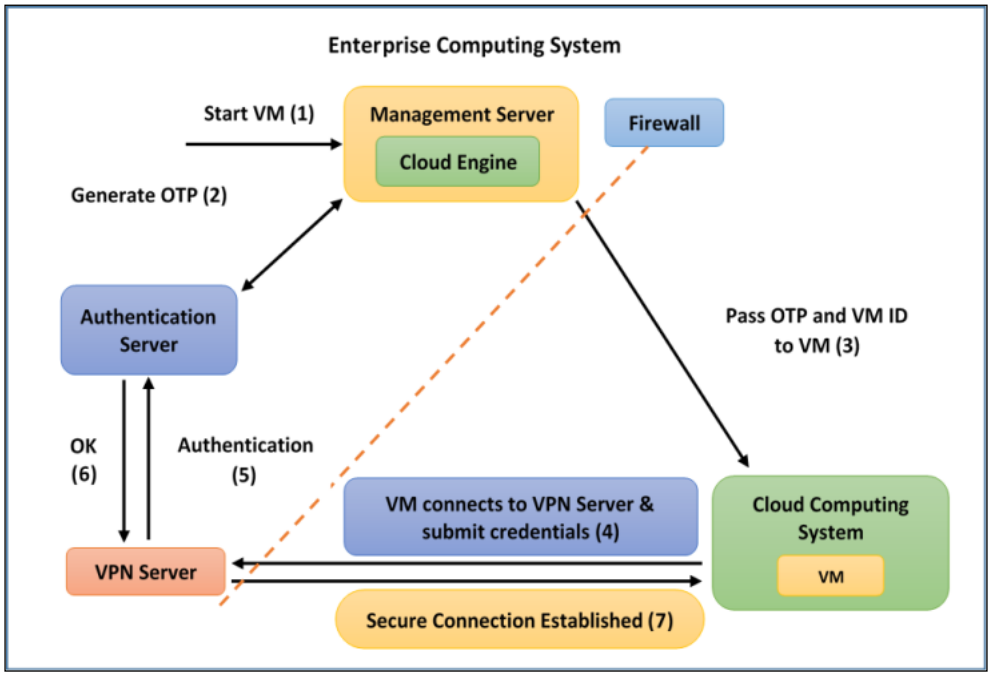

Figure 4. Flow Chart of OTP based Algorithm

4. Result

The above algorithm is tested in a simulation environment where a private cloud having five machine acting one machine as server and rest as client machines. On client machine virtual machine are created using image having Ubuntu 14.04.4. Java version SE 7 is used to create the interfaces required to login to the server and to authenticate the user of the virtual machine. Also database is maintained using My SQL to store the VM id and the MAC address pair. An OTP is generated and send to the host machine whenever virtual machine wants to connect with the server to make security of virtual machine image. After validating the information of the virtual machine (VM id, MAC address of the machine) there can be access of virtual machine image to make instances.

5. Conclusion & Future Scope

Virtual image security is important in cloud computing paradigm. Security involves access control, integrity, confidentiality, Malware protection, Auto update patching. In the above discussed security scheme no one provides all the security parameters to be fulfilled. Although Mirage Image management system speeds up image deployment and supports advanced features such as version control, fast offline operations, efficient search, image comparison, and other analyses of image, it has the limitation of not having accurate filters and does not eliminate the risk entirely. EVDIC security approach satisfies most of the security parameters. Most of them are used for dormant images (not running). In future it would be suggest that there should be more powerful security scheme which covers all the issues and threats of security to be resolved. Also the algorithm can be tested in hybrid environment.

References

[1] Hashizume, K., Rosado, D. G., Fernández-Medina, E., & Fernandez, E. B. (2013). An analysis of security issues for cloud computing. Journal of Internet Services and Applications, 4(1), 1.
[2] Wei J, Zhang X, Ammons G, Bala V, Ning P (2009) Managing Security of virtual machine images in a Cloud environment. In: Proceedings of the 2009 ACM workshop on Cloud Computing Security. ACM New York, NY, USA, pp 91–96
[3] Owens, K. (2009). Securing virtual compute infrastructure in the cloud. Whitepaper. SavvisCorp.[Online]. Available: http://www. savvis. com/en-us/info% 5Fcenter/documents/hos-whitepaper securing virtual compute infrastructure in the cloud. pdf.
[4] Grobauer, B., Walloschek, T., & Stocker, E. (2011). Understanding cloud computing vulnerabilities. IEEE Security & Privacy, 9(2), 50-57.
[5] Almorsy, M., Grundy, J., & Müller, I. (2010, November). An analysis of the cloud computing security problem. In Proceedings of APSEC 2010 Cloud Workshop, Sydney, Australia, 30th Nov.
[6] Jansen, W. A. (2011, January). Cloud hooks: Security and privacy issues in cloud computing. In System Sciences (HICSS), 2011 44th Hawaii International Conference on (pp. 1-10). IEEE.
[7] Wei, J., Zhang, X., Ammons, G., Bala, V., & Ning, P. (2009, November). 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.
[8] Kazim, M., Masood, R., & Shibli, M. A. (2013, November). Securing the virtual machine images in cloud computing. In Proceedings of the 6th International Conference on Security of Information and Networks (pp. 425-428). ACM.
[9] Schwarzkopf, R., Schmidt, M., Strack, C., Martin, S., & Freisleben, B. (2012). Increasing virtual machine security in cloud environments. Journal of Cloud Computing, 1(1), 1-12.
[10] Jeswani, D., Verma, A., Jayachandran, P., & Bhattacharya, K. (2013, July). ImageElves: rapid and reliable system updates in the cloud. In Distributed Computing Systems (ICDCS), 2013 IEEE 33rd International Conference on (pp. 390-399). IEEE.
[11] Ali, M., Khan, S. U., & Vasilakos, A. V. (2015). Security in cloud computing: Opportunities and challenges. Information Sciences, 305, 357-383.
[12] Fan, K., Mao, D., Lu, Z., & Wu, J. (2013, June). Ops: Offline patching scheme for the images management in a secure cloud environment. In Services Computing (SCC), 2013 IEEE International Conference on (pp. 587-594). IEEE.
[13] Zhang, F., Huang, Y., Wang, H., Chen, H., & Zang, B. (2008, October). PALM: security preserving VM live migration for systems with VMM-enforced protection. In Trusted Infrastructure Technologies Conference, 2008. APTC'08. Third Asia-Pacific (pp. 9-18). IEEE.
[14] Garfinkel, T., & Rosenblum, M. (2005, May). When virtual is harder than real: Security challenges in virtual machine based computing environments. In HotOS.
[15] Zhou, W., Ning, P., Zhang, X., Ammons, G., Wang, R., & Bala, V. (2010, December). Always up-to-date: scalable offline patching of vm images in a compute cloud. In Proceedings of the 26th Annual Computer Security Applications Conference (pp. 377-386). ACM.
[16] Bleikertz, S., Schunter, M., Probst, C. W., Pendarakis, D., & Eriksson, K. (2010, October). Security audits of multi-tier virtual infrastructures in public infrastructure clouds. In Proceedings of the 2010 ACM workshop on Cloud computing security workshop (pp. 93-102). ACM.
[17] Studnia, I., Alata, E., Deswarte, Y., Kaaniche, M., & Nicomette, (2012, November).Survey of security problems in cloud computing virtual machines. In Computer and Electronics security Applications Rendez-vous (C&ESAR 2012).Cloud and security: threat or opportunity (pp. p-61).
[18] https://www.usenix.org/legacy/event/hotcloud11/tech/final_files/Ammons.pdf
[19] http://docs.openstack.org/imageguide/content/ch_introduction.html.
[20] http://www.webopedia.com/TERM/N/network_virtualization_NV.html.

