Cloud Computing Architectures Based IDS

En Niari Saad*, Khalil El Mahdi*
National Higher School of Computer Science and Systems Analysis (ENSIAS)
Information Security Research Team (ISeRT)
University of Mohammed V, Rabat, Morocco
{saad.enniari, elmahdi.khalil}@um5s.net.ma

Mostapha Zbakh
National Higher School of Computer Science and Systems Analysis (ENSIAS)
Information Security Research Team (ISeRT)
University of Mohammed V, Rabat, Morocco
zbakh@ensias.ma

Abstract—**Today, cloud computing is an attractive and cost-saving service for buyers as it provides accessibility and reliability options for users and scalable sales for providers. Before implementing this method of computing, however, it is important to consider the security of the cloud. In this paper, we will present, a classification of specific and traditional attacks to the cloud computing according to their origin and their category, as a solution to protect the cloud from these attacks, the IDS integrated in the cloud remains among the best solution, therefore we will show some existing cloud computing architecture based Intrusion Detection System (IDS), their strengths and weaknesses. For the comparative study between the architectures, we have adopted transparency, alerts analysis, authentication, accountability, dynamic reaction, centralized management, interoperability, deployability and control from front office side as criterion for comparison, as a result of this comparative study, we propose a new architecture in one hand by correcting some weaknesses and in the other hand integrating certain concept.**

Keywords-component: intrusion detection; intrusion prevention; cloud computing; computer attacks; network attacks; cloud security.

I. INTRODUCTION

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction [1].

Cloud computing is seen by many as the next wave of information technology for individuals, companies and governments, developing a cloud strategy is a high priority for 81% of companies [2], although security is one of the major issues which hamper the growth of cloud.

The risks identified in the assessment of cloud computing are classified into three categories [3]:

- Policy and organizational.
- Technical.
- Legal.

Intrusion detection is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents, which are violations or imminent threats of violation of computer security policies, acceptable use policies, or standard security practices [4].

Intrusion detection system can be categorized in three types of IDS technologies:

- Network-Based, which monitors network traffic for particular network segments or devices and analyzes the network and application protocol activity to identify suspicious activity;
- Host-Based, which monitors the characteristics of a single host and the events occurring within that host for suspicious activity;
- VM-based, which monitors the characteristics of virtual machines.

The rest of the paper is organized as follows. Section 2 describes the state of the art of attacks in the cloud environment, in section 3 based on the taxonomy of IDS we'll provide definitions and state of the art of IDS/IPS. Section 4 provides three architectures of cloud computing based IDS, a comparative study between these architectures will be presented in section 5. After that in Section 6, we list some possible future works, and we gives a short summary of our contribution.

II. ATTACKS IN THE CLOUD COMPUTING

In Figure 1 [5] a service provider (SP) runs one or more service instances (SI) on the cloud, which can be accessed by a group of final service user (SU). For this purpose, the SP hires resources from the cloud provider (CP). It is worth noticing that the SU and SP do not have any physical control over cloud machines, whose status cannot be observed.

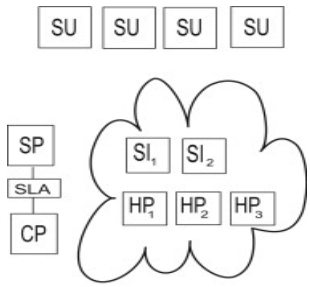

Figure 1. Cloud service model components

978-1-4673-4766-2/12/$31.00 ©2012 IEEE

Possible attacks against cloud system scan are classified as follows [10]:

- **CAT1** Resource attacks against CS.
- **CAT2** Resource attacks against PS.
- **CAT3** Data attacks against CPs.
- **CAT4** Data attacks against SPs.
- **CAT5** Data attacks against SU.

Resource attacks (CAT1-CAT2) regard the misuse of resources, such as stealing virtual resources to mount a large scale botnet attack. Data attacks (CAT3-CAT4) steal or modify service or node configuration data (that can be used later to perform an attack). Data attacks against service users (CAT5) can lead to leakage of sensitive data. CAT1 and CAT3 attack classes involve an attack to cloud infrastructure components. Virtualization technologies underlying cloud computing infrastructure can pose security challenges themselves.

A. Intrusions to Cloud Systems

There are several attacks affecting availability, confidentiality and integrity of Cloud resources and services. These attacks can be originated from [1]:

- **ORG1** Outside the cloud.
- **ORG2** Sibling VMs.
- **ORG3** VMs.

Whereas victims can be the providers running services in the cloud (CAT2-CAT4), the cloud infrastructure itself (CAT1-CAT3) or other users (CAT5). A traditional threat is when an attacker attempts to perform remote exploitation of software vulnerabilities in the guest system (CAT2). Some attacks are made possible by exploiting cloud services (CAT1-CAT2), since a malicious party can legally hire other instances within the cloud and, it can manage to learn confidential information (CAT5). Other attacks are also possible such as Denial of Service (CAT1-CAT2), estimating traffic rates, and keystroke timing (CAT2-CAT5) [5, 6].

B. Attacks Taxonomy

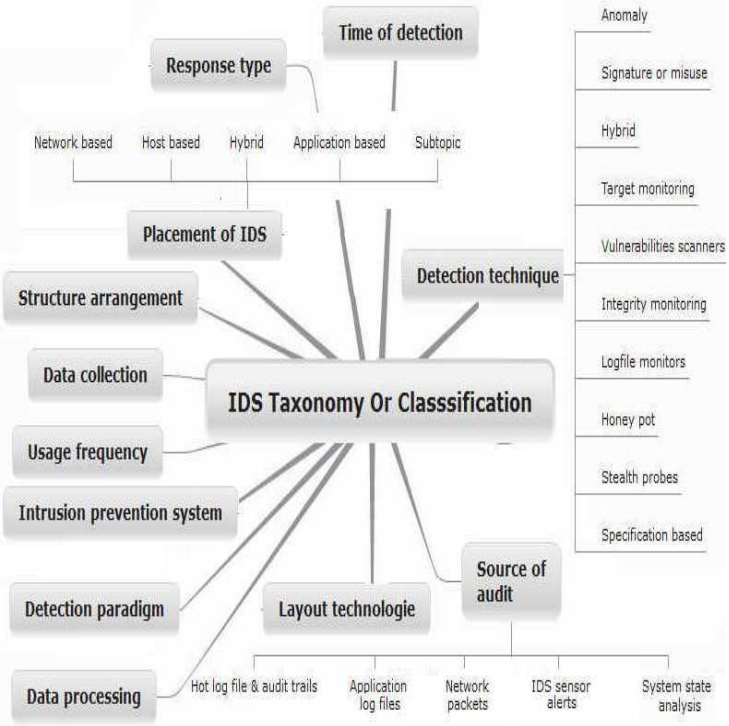

Figure2. IDS Taxonomy

The original purpose of the taxonomy was to reduce the number of attacks needed for the evaluations. Instead of developing a large number of attacks, it should be sufficient to pick a representative subset of each category of attacks [14].

Based on existing taxonomies we distinguish [7] several classes of attacks according to their attributes: attack objective, attack effect, attack automation, attack service, target, and OSI level vulnerability type.

In the rest of the paper our work will be based on class objective by considering the following types of attacks:

- Super-user privilege gain.
- User privilege gain; Denial of service.
- Information integrity violation.
- Information resource confidentiality violation; Malicious code execution.
- Security policy violation.

To cover aspects of cloud computing we will add other types of specific attacks like:

- Attack in virtual machine or hypervisor.
- Backdoor channel.

In Table I, we classify the attacks in a cloud environment by origin and category as defined in previous chapters.

TABLE I. CLASSIFICATION OF ATTACKS BY ORIGIN AND CATEGORY

Origin / Category	*ORG1*	*ORG2*	*ORG3*
CAT1	Dos (DDOS) Backdoor Channel User/Root privilege gain Malicious code execution Information resource confidentiality violation Information integrity violation	Dos (DDOS) Attack in vm/hyp Backdoor Channel User/Root privilege gain Malicious code execution Information resource confidentiality violation Information integrity violation	Dos (DDOS) Attack in vm/hyp Backdoor Channel User/Root privilege gain Malicious code execution Information resource confidentiality violation Information integrity violation
CAT2	Dos (DDOS) Backdoor Channel User/Root privilege gain Malicious code execution Information resource confidentiality violation Information integrity violation	Dos (DDOS) Attack in vm/hyp Backdoor Channel User/Root privilege gain Malicious code execution Information resource confidentiality violation Information integrity violation	Dos (DDOS) Attack in vm/hyp Backdoor Channel User/Root privilege gain Malicious code execution Information resource confidentiality violation Information integrity violation
CAT3	Backdoor Channel User/Root privilege gain Malicious code execution Information integrity violation	Attack in vm/hyp Backdoor Channel User/Root privilege gain Malicious code execution Information integrity violation	Attack in vm/hyp Backdoor Channel User/Root privilege gain Malicious code execution Information integrity violation
CAT4	Backdoor Channel User/Root privilege gain Malicious code execution Information integrity violation	Attack in vm/hyp Backdoor Channel User/Root privilege gain Malicious code execution Information integrity violation	Attack in vm/hyp Backdoor Channel User/Root privilege gain Malicious code execution Information integrity violation
CAT5	Backdoor Channel User/Root privilege gain Malicious code execution Information integrity violation	Attack in vm/hyp Backdoor Channel User/Root privilege gain Malicious code execution Information integrity violation	Attack in vm/hyp Backdoor Channel User/Root privilege gain Malicious code execution Information integrity violation

III. IDS AND IPS IN CLOUD COMPUTING

A. IDS taxonomy

The taxonomy provided in Figure 2 [8] presents an up-to-date Intrusion Detection System classification.

Since we are working on the integration of IDSs in cloud computing we'll consider for the rest of this paper the classification of IDS according to their protected system or placement.

B. Host Based IDS

Host-based systems were the first type of IDS to be developed and implemented. These systems collect and analyze data that originate on a computer that hosts a service, such as a Web server. One example of a host-based system is programs that operate on a system and receive application or operating system audit logs. These programs are highly effective for detecting insider abuses [9].

C. Network Based IDS

Network-based intrusion detection analyzes data packets that travel over the actual network. These packets are examined and sometimes compared with empirical data to verify their nature: malicious or benign. Because they are responsible for monitoring a network, rather than a single host, NIDS tend to be more distributed than host-based IDS [9].

D. Hybrid IDS

A hybrid system that incorporates both network and host based IDSs will be advantageous if the network IDS filters alerts and notifications in an identical manner to the host based portion of the system. In such hybrid systems the IDS mainly rely on the host based components and uses the network based IDS to complete the defense [8].

In addition of NIDS, HIDS and Hybrid IDS, presented in class "Protected System or Placement of IDS" we can add another new type of IDS named Virtual Machine Introspection IDS (VMI IDS) or Hypervisor based IDS that bring together advantages of HIDS and NIDS that we'll detail in the following chapter.

E. Virtual Machine Introspection (Hypervisor Based) IDS

If the IDS reside on the host, it has an excellent view of what is happening in that host's software, but is highly susceptible to attack. On the other hand, if the IDS resides in the network, it is more resistant to attack, but has a poor view of what is happening inside the host, making it more susceptible to evasion. Hypervisor based IDS retain the visibility of host-based IDS, but pull the IDS outside of the host for greater attack resistance. We achieve this through the use of a virtual machine monitor VMM or hypervisor. Using this approach allows us to isolate the IDS from the monitored host but still retain excellent visibility into the host's state. The VMM also offers us the unique ability to completely mediate interactions between the host software and the underlying hardware [10].

F. Intrusion Prevention System (IPS)

An IPS is any hardware or software device that has the ability to detect and prevent known attacks. Currently there are two types of IPSs: host-based and network-based.

The IPS's software for host-based systems will be installed directly on servers that host the monitored applications. All IPS for network-based systems is specifically targeted at detecting

And then preventing publicly known application-specific attacks [8].

G. Location of IDS in the cloud

Since IAAS is most flexible model for Intrusion Detection (ID) deployment. Unlike the other two, IaaS gives a consumer more options. We can identify four spots [16].

a) In the virtual machine (VM) itself: Deploying ID in the VM allows you to monitor the activity of the system, and detect and alert on issues that may arise.

b) In the hypervisor or host system: Deploying ID in the hypervisor allows you to not only monitor the hypervisor but anything travelling between the VMs on that hypervisor. It is a more centralized location for ID, but there may be issues in keeping up with performance or dropping some information if the amount of data is too large. Furthermore, this space is very immature at this time.

c) In the virtual network: Deploying ID to monitor the virtual network (i.e., the network established within the host itself) allows you to monitor the network traffic between the VMs on the host, as well as the traffic between the VMs and the host. This "network" traffic never hits the traditional network.

d) In the traditional network deploying: ID here allows you to monitor, detect, and alert on traffic that passes over the traditional network infrastructure

H. Responsibility of IDS in the cloud

One thing to confirm right away is who will be responsible, and how they will be responsible, for IDS in the cloud [16].

- Providers will deploy ID in certain locations that feed into their (not consumer) IDS.
- Consumer must have a service-level agreement (SLA) in place that require providers to notify him if he is affected directly (i.e., they see attacks against consumer VMs) or indirectly (i.e., they see attacks against a hypervisor that is running consumer VMs).
- If and when client deploy ID, it should integrate (in some manner) into current monitoring and alerting client infrastructure.
- It is likely that the future will have third parties that provide IDS for the cloud, and that this will just be an add-on cost for those who do not want to manage ID in their cloud instances.

Now we'll consider the following three IDSs options [16]:

a) HIDS: Can be deployed in the VM, as well as the host/hypervisor. The HIDS on the VM would be deployed, managed and monitored by client. The HIDS on the hypervisor would be the responsibility of IaaS provider.

b) NIDS: This type of deployment is useful in detecting some attacks on the VMs and hypervisor. It does, however, have several limitations. The first is that it cannot help when it comes to attacks within a virtual network that runs entirely within the hypervisor. Second, it has very limited visibility into the host itself. Lastly, if the network traffic is encrypted, there is really no effective way for the NIDS to decrypt the traffic for analysis. In the cloud, NIDS falls completely in the realm of the provider to deploy and manage.

c) Hypervisor-based IDS: The third option would be the use of an intrusion detection system that runs at the hypervisor layer but is not strictly a HIDS for the hypervisor. One of the promising technologies in this area is the use of VM introspection [15]. This type of IDS allows you to monitor and analyze communications between VMs, between hypervisor and VM and within the hypervisor based virtual network. The advantage of hypervisor-based ID is the availability of information, as it can see basically everything. The disadvantage is that the technology is new and you really need to know what you are looking for. As with NIDS, this falls completely within the scope of the provider to deploy and manage.

TABLE II. COMPARATIVE TABLE OF PROTECTED SYSTEM IDS

Network IDS (NIDS) • Poor view. • Good resistance to attacks.	User-space • HIDS Good view. • Zero resistance to attacks.
Kernel-space HIDS • Program user can change changer kernel. • IDS crash because the systems fail open.	VMI IDS • Good resistance to attacks. • Need of OS interface library that provides an OS-level view of the VM by interpreting the hardware state.

Table above shows a comparison between IDS by highlighting the advantages and disadvantages of each.

IV. ARCHITECTURE OF CLOUD COMPUTING BASED IDS

In this section we present three architectures of cloud computing-based IDS and in the next section we will provide a comparative study between them.

A. First Architecture

Figure 3 shows a possible deployment of IDS in the Cloud infrastructure. Each virtual component should be secured by a separated IDS sensor, which is responsible for one virtual machine and can be configured by the Cloud user. This sensor should monitor the virtual components based on the requirements of the user.

For each layer, there should be Network based sensors and Host-based sensors deployed accordingly.

Additionally, the IDS sensor should report alerts to a central IDS management system, which is responsible to gather and preprocess the alerts of all sensors. Cloud users can view and configure their sensors by using the IDS Management system [11].

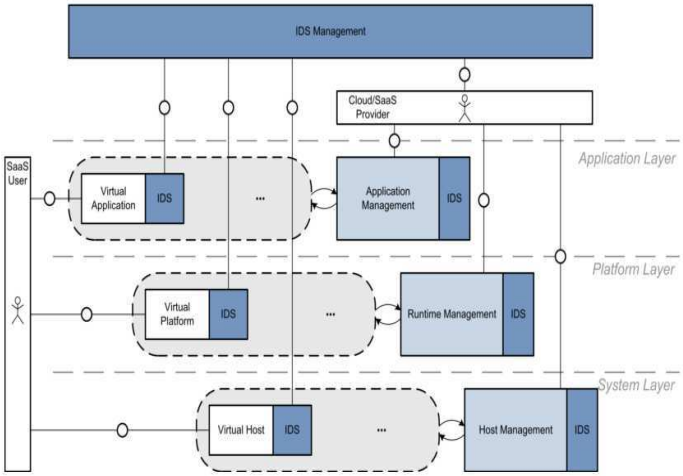

Figure 3. Overall deployment of IDS in cloud computing architecture

To implement the architecture described above with virtual machine the authors propose the system shown in (Figure 4).

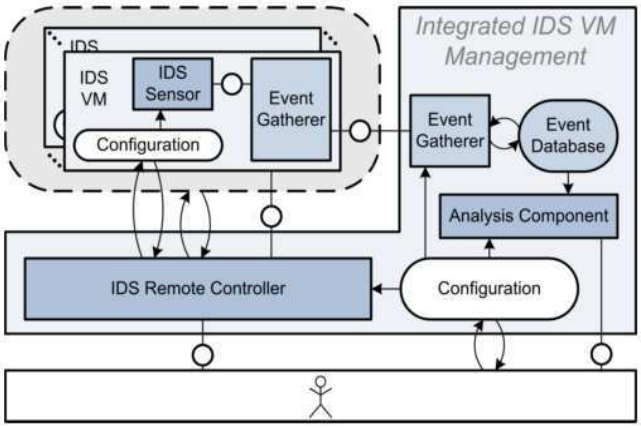

Figure 4. Architecture of VM-integrated IDS Management

It includes several IDS Sensor VMs and an IDS Management Unit. The IDS Management Unit consists of four active components: Event Gatherer, Event Database, Analysis Component, and IDS Remote Controller. The Event Database is a passive storage that holds information about all received events. It can be accessed through the Analysis Component. User controls the IDS management through direct interaction and configuration of the core components. The IDS Sensors on the VMs are responsible for detecting and reporting malicious behaviors. Each sensor is connected to the Event Gatherer component to transmit triggered events. A sensor, which could be a running NIDS with all its signatures and configurations, can be configured through the IDS Remote Controller [11].

B. *Second Architecture*

In figure 5 the author [12] proposed a data mining technique that could potentially prove to be beneficial to IDSs. The idea is to use biclustering as a tool to analyze network traffic and enhance IDSs. Bi-clustering is the problem of finding a partition of the vectors and a subset of the dimensions such that the projections along those directions of the vectors in each cluster are close to one another. The problem requires the clustering of the vectors and the dimensions simultaneously.

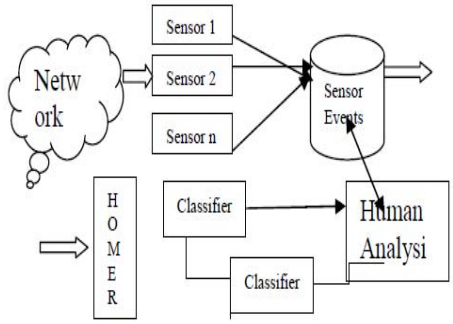

Figure 5. Overall intrusion detection system based on data mining

C. *Third Architecture*

Rapid And Proactive Vulnerabilities Scanning (RPVS) [13] is analogous to NAC (Network Admission Control) commonly implemented at the Network Router level to identify and quarantine new hardware systems, till they are thoroughly scanned for vulnerabilities.

RPVS; showed in figure 6; will detect Operating system, in the domain (range of IP addresses of an enterprise), seamlessly, quarantines it, and also scans for OS, user, data, privileges, and OS vulnerabilities. the Approach is based on the premise that an OS, may have very critical/confidential data like SSN, Credit Card info, etc., and so the schema/metadata have to be checked before allowing users access to it, to prevent malicious users accessing confidential data.

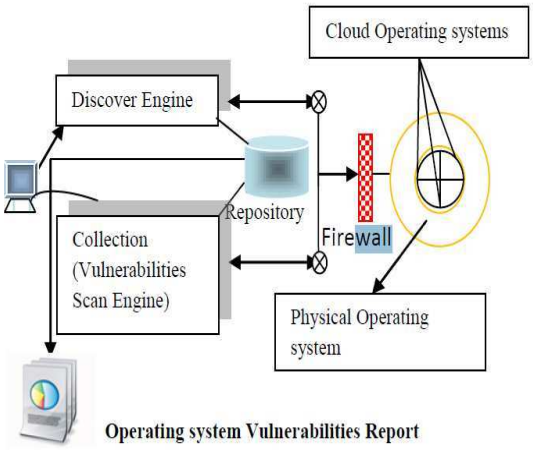

Figure 6. RPVS System Modules

- Scanning of ports.
- Identification of vulnerabilities.
- Generation of reports and validation of the state of security of the information technology infrastructure.

V. COMPARATIVE STUDY

We present below in table 3 a summary of the features provided by each architecture, we note that the first architecture is the most efficient despite the lack of transparency, dynamic reaction, and accountability, the second architecture does not provide good distributions of IDS environment in the cloud, for the third architecture it focuses only on the analysis of the operating system making it less efficient cover them for all types of attacks.

TABLE III. COMPARATIVE STUDY OF CLOUD BASED IDS ARCHITECTURES

	Arch I	Arch II	Arch III
Transparency	Missing	Missing	Medium
Alerts analysis	OK	OK	Missing
Authentication	OK	Medium	Medium
Accountability	Missing	Medium	Missing
Dynamic reaction	Missing	Missing	Missing
Centralized management	OK	OK	Medium
Interoperability	OK	OK	OK
Deployability	OK	Medium	OK
Control from front office side	OK	OK	OK

VI. CONCLUSION AND FUTURE WORKS

In this paper we have presented the state of the art of attacks in cloud environment; we distinguish several classes of attacks according to their attributes: attack objective, attack effect, attack automation, attack service, target, and OSI level vulnerability type, after that we presented an up-to-date Intrusion Detection System classification, following this classification we have proposed a comparative study on architecture based IDS in cloud computing environment, according to the following criteria: transparency, alerts analysis, authentication, accountability, dynamic reaction, centralized management, interoperability, deployability, and control from front office side.

We are currently deploying the three architectures to measure the effectiveness and accuracy of attacks detection.

As a future research work, we plan to base on the first architecture to provide a more efficient architecture, we thought that is possible to enhance the transparency, dynamic reaction, and accountability by integrate the virtual machine introspection instead of HIDS.

Another interesting area of research is to design architecture-based IDS which consider the Multi-Tenancy, the philosophy of integration and deployment of IDS in cloud should be changed, therefore each business unit must be controlled separately for each user to improve policy-driven enforcement, segmentation, isolation and governance in cloud computing environment.

REFERENCES

[1] Forrester 2012 Cloud Survey http://www.bmc.com/industry-analysts/reports/forrester-2012-cloud-survey.html (accessed Mai 2012).

[2] National Institute of Standards and Technology (NIST) http://www.nist.gov/itl/csd/cloud-102511.cfm (accessed Mai 2012).

[3] Cloud computing benefits, risks and recommendations for information security by ENISA http://www.ensia.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment.

[4] Security Guidance for Critical Areas of Focus in Cloud Computing V2.1 by Cloud Security Alliance 2009 https://cloudsecurityalliance.org.

[5] Roschke, S., Cheng, F., Meinel, Ch., "An Advanced IDS Management Architecture", In Proceedings of 6th Information Assurance and Security Conference (IAS'10), IEEE, August 2010.

[6] Sherish Johri, "Novel Method for Intrusion Detection using Data Mining",In:International Journal of Advanced Research in Computer Science and Software Engineering, April 2012.

[7] S. Ramachandran, A. Ramachandran, "Rapid and Proactive Approach on Exploration of Vulnerabilities in Cloud based Operating Systems", International Journal of Computer Applications (0975 – 8887) Volume 42– No.3, March 2012.

[8] Karen Scarfone and Peter Mell, "Guide to Intrusion Detection and Prevention Systems (IDPS)", Recommendations of the National Institute of Standards and Technology (NIST), Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology Gaithersburg, MD 20899-8930, February 2007.

[9] Flavio Lombardi, Roberto Di Pietro, "Secure virtualization for cloud computing", Volume 34, Issue 4, Pages 1113–1122, July 2011.

[10] M. Smith, T. Friese, M. Engel, B. Freisleben, "Countering security threats in service-oriented on-demand grid computing using sandboxing and trusted computing techniques", J. Parallel Distrib. Comput., 66 (9), pp. 1189–1204, 2006.

[11] Chirag Modi, Dhiren Patel, Bhavesh Borisaniya, Hiren Patel, Avi Patel, Muttukrishnan, "A survey of intrusion detection techniques in Cloud", 2012.

[12] IEEE COMPUTER AND RELIABILITY SOCIETIES, "Understanding Cloud Computing Vulnerabilities", 2011.

[13] Suhair Hafez Amer, John A. Hamilton, Jr., Intrusion Detection Systems (IDS) Taxonomy - A Short Review http://journal.thedacs.com/issue/54/163.

[14] N. Paulauskas, E. Garšva, "Computer System Attack Classification", Journal of Electronics and Electrical Engineering. – Kaunas: Technology, No. 2(66). – P. 84–87, 2006.

[15] Tal Garfinkel, Mendel Rosenblum, "A Virtual Machine Introspection Based Architecture for Intrusion Detection", Proceedings of the Internet Society's 2003, Symposium on Network and Distributed System Security, 2003

[16] Phil Cox, "Intrusion detection in a cloud computing environment" http://searchcloudcomputing.techtarget.com/tip/Intrusion-detection-in-a-cloud-computing-environment.