Cloud Service Feature driven Security Policies for Virtualized Infrastructures

Ramaswamy Chandramouli
National Institute of Standards & Technology
Gaithersburg, MD, USA
mouli@nist.gov

ABSTRACT

With the increasing maturity of various cloud service delivery models (Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS)) and deployment models (Private, Community, Public, Hybrid), the security risk profile of each cloud service configuration is coming into focus. In this paper, we take up the example of a Public Infrastructure as a Service (Iaas) cloud provider who provides computing services through a data center with a virtualized infrastructure. In order to provide the needed security assurance for its IaaS cloud offering, the cloud provider needs to implement various security measures as part of the infrastructure configuration. A precursor to developing security measures is a comprehensive security policy. Now these policies are dependent upon the set of service features that the IaaS cloud provider provides as part of its offering as well as internal administrative capabilities needed to support those features. The focus of this paper is to illustrate an approach for derivation of appropriate security policies based on the security goals of functions associated with internal administration capabilities and cloud service features.

Keywords - Cloud computing, Infrastructure as a Service, Public cloud, Security Policy, Virtualization.

1. INTRODUCTION

The security risk profile of a cloud service is dictated by the following factors. We call the variables associated with these factors are Cloud Service Orchestration variables.

- Cloud Delivery Model (Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS)) [1]
- Cloud Deployment Model (Private, Hybrid, Community, Public)
- The functional capabilities offered by the Cloud Service Provider (we call this as Service Feature Set in this paper) and
- The Technologies used to enable the functional capabilities (e.g., Virtualization, Federation Protocols etc)

A given cloud service, therefore, is defined in terms of the values of the applicable cloud service orchestration variables from the above factors. Out of the above four factors, once the cloud delivery model and cloud deployment model is chosen, the detailed security risk analysis and the security threats are entirely dictated by the functional capabilities offered by the cloud service provider and the underlying technology used in the IT infrastructure used by the cloud service provider to enable those functional capabilities that constitute the service package.

The cloud service that is the focus of this paper has Infrastructure as a Service (Iaas) as the cloud delivery model and Public Cloud as the Cloud deployment model. The main cloud technology we consider is virtualization [2]. We also consider a comprehensive set of functional capabilities that can be provided based on the current state of virtualization technology and market orientation.

It must be mentioned that not every IaaS cloud offering has to be enabled only using virtualization technologies. The economic viability of an IaaS is in large part enhanced due to abstraction of resources (computing, storage and network) and virtualization technology is the most prevalent one used today for providing that abstraction.

Now, based on the description of the our reference cloud service, it should be clear that the cloud service provider scenario we are referring to is an IaaS cloud provider who provides storage and computing services through a data center with a virtualized infrastructure. The use of a virtualized infrastructure by an IaaS provider makes the most economic sense because of the following:

- IaaS cloud provider is able to utilize the entire set of computing, storage and network equipment in an optimum fashion with high level of utilization.
- IaaS cloud provider is able to quickly ramp up the resources with minimal re-configuration whenever the demand from the existing cloud subscribers increases or new subscribers join the service. [3]
- IaaS is able to offer diversity in terms of computing power/throughput (through custom configuration of Virtual Machines) as well as platform diversity (e.g., different operating systems).

Once the IaaS cloud service provider takes care of the adequacy of the resources (computing, storage and networking capabilities), the next two critical issues are:

- Service Management
- Security (Adequate protection for cloud subscriber's data and application) [4]

In order to offer a robust and secure IaaS cloud offering, the cloud provider has to have the following:

- A set of administrative capabilities relating to the virtualized infrastructure in its data center.
- A set of features that is part of the cloud service that the cloud provider offers which the cloud subscriber is able to invoke based on its subscription package.

In order that the internal virtualized infrastructure of the IaaS cloud provider is secure and the service orchestration/configuration maintains its integrity, there needs to be a set of security policies associated with each internal administrative capability as well as with a cloud service feature. The purpose of this paper is to enumerate these internal administrative capabilities (IAC) and cloud service features (CSF), analyze the security goal associated with each and then provide a statement or scope of security policies that should go with each administrative capability or cloud service feature. The enumeration is based on the author's analysis of the current state of virtualization technology deployed in commercial IaaS cloud service offerings as well as common subscriber-facing service features currently available in those offerings.

The need for strong security measures and hence a comprehensive set of security policies is much more critical for protecting virtualized infrastructures owned/operated by cloud providers compared to virtualized infrastructures deployed as part of the enterprise IT architecture [5]. This is due to the fact that enterprise users who are cloud service subscribers have shifted their trust from the IT resources in their data centers to IT resources under the control of cloud providers. This trust is needed for satisfying the internal audit requirements as well as public regulatory compliance needs for enterprise IT users.

Before we provide the organization of this paper, a note regarding certain naming conventions used in this paper is in order. The following are the conventions used:

- IAC-Fx – denotes function Fx (x being the running sequence) associated with Internal Administration Capability
- IAC-SPx – denotes security policy SPx associated with Internal Administrative Capability
- CSF-Fx – denotes function Fx associated with Cloud Service Feature
- CSF-SPx – denotes security policy SPx associated with Cloud Service Feature

The organization of the rest of the paper is as follows. In sections 2 through 5 we look at the administrative capabilities (IAC-F1 through IAC-F8) (both technical and procedural) required for an IaaS cloud provider to provide security for its virtualized infrastructure and derive the associated security policies (IAC-SP1 through IAC-SP8). In sections 6 through 9, we describe the various features that an IaaS cloud provider could offer as part of its service package (CSF-F1 through CSF-F15) and the security policies associated with each of those service features (CSF-SP1 through CSF-SP15). Section 10 provides the conclusions and benefits.

2. FEATURES AND POLICIES RELATING TO PROTECTION OF VIRTUALIZED HOSTS

A physical host on which is mounted a Virtual Machine Monitor (VMM) or Hypervisor is called a Virtualized Host. A Virtualized host is capable of supporting multiple Virtual Machines (VMs) each with its own operating system (called a Guest O/S).

A virtualized host is the basic building block of the virtualized infrastructure of an IaaS cloud service provider. It is also the foundational resource offered in the service since cloud subscribers define their service entities (i.e., virtual machines or VMs) on it. Hence adequate protection for all virtualized hosts is critical for the security of the entire IaaS cloud service. With this as the driving security goal, we have to look at the set of administrative capabilities or functions that are needed to realize it.

In a datacenter set up for a public IaaS cloud service, the cloud provider organization needs to provide direct access to virtualized hosts only for a limited set of users who need to manage and/or monitor the virtualized infrastructure elements such as the Virtual Machines, Virtual Security Appliances and Virtual Networks.

This may require the following functions:
IAC-F1: The users accessing a virtualized host should be authenticated using a robust authentication mechanism
IAC-F2: The means of user and network accesses to the virtualized hosts should be tightly controlled.
IAC-F3: To perform management functions on a virtualized host (such as monitoring of inter-VM traffic), a virtual network must be setup inside a virtualized host (hypervisor specifically).

The security policies associated with the above functions based on the state of the technology are as follows:
IAC-SP1: Authentication policies should call not only for robustness in some selected virtualized hosts but also some uniformity and consistency across all virtualized hosts. This may require that authentication of users into individual virtualized hosts be integrated with a directory service (e.g., Active Directory) using a secure protocol (e.g., Kerberos) so as to define and enforce consistent authentication policies.
IAC-SP2: Access policies relating to user and network access to virtualized hosts should cover designation of users/secure channels for remote access (e.g., SSH), designation of client nodes (e.g., TCP Wrappers) and designation of allowable in-bound and out-bound communication ports (e.g., through firewall rules)[6].
IAC-SP3: The virtual network in the hypervisor should be configured such that there is a dedicated management network. This is often accomplished by having a dedicated virtual switch inside a hypervisor connect to a dedicated physical network adapter/network interface card on the host.

3. FEATURES AND POLICIES RELATING TO CREATION & STORAGE OF VIRTUAL MACHINE IMAGES

Many of the IaaS cloud providers offer a set of virtual machine (VM) images for use by their subscribers to create and launch VM instances. The following are the administrative capabilities required if the IaaS cloud provider offers this feature:
IAC-F4: The cloud providers should have tools to create secure VM images.
IAC-F5:The cloud provider should provide a means to securely store the VM images in a Image Repository
IAC-F6:The cloud provider should maintain the security status of VM images in the Image Repository

The corresponding security policies required to support the above capabilities are given below:
IAC-SP4: The IaaS cloud provider should develop security baselines for various types of VM Images it wants to offer to cloud subscribers. These baselines should cover Guest OS versions, configuration values and anti-malware software.

IAC-SP5: The IaaS cloud provider should ensure that only authorized administrators can access, create, store or replace VM images in the image repository.
IAC-SP6: The IaaS cloud provider should have policies for periodically scanning and updating the VM images through operations such as patch application, configuration changes or updating anti-malware signatures.

4. FEATURES AND POLICIES RELATING TO MANAGMENT OF VIRTUALIZED INFRASTRUCTURE

Having looked at the administrative capabilities and policies governing secure access to virtualized hosts, the next step is configuration of privileges and permissions needed for the management of the entire virtualized infrastructure. The management functions that can be performed from the individual virtualized hosts are limited to those that pertain to virtual machines residing on that host. In most practical infrastructures owned by the IaaS cloud provider, a scalable and efficient management process takes place through a centralized management server [6] that has visibility into multiple virtualized hosts.

Some of the functions related to management of entire virtualized infrastructure are stated below:
IAC-F7: The cloud provider should have tools and capabilities for performing key management functions on the virtualized infrastructure such as: (a) Creation of a cluster consisting of a group of virtualized hosts and (b) Balancing the workload among the hosts within a cluster by having the capability to perform live VM migration across the hosts within the cluster.

The policies associated with the above privilege management functions are:
IAC-SP7: (a) The cloud provider should limit the capability to perform management functions on the virtualized infrastructure to a selected set of qualified administrators (b) The permissions should be granular and their assignment to authorized administrators should be based on principles such as Least Privilege, Separation of Duty etc and (c) The integrity and efficiency of permission assignment process should be improved by encapsulating related set of permissions into a role with meaningful names and using the roles as the basis for allocation to administrative users.

5. FEATURES AND POLICIES RELATING TO OPERATIONAL PROCESSES AND PROCEDURES

Cloud subscribers may be hosting data on an IaaS cloud provider's infrastructure whose creation, protection and dissemination are subject to public regulations such as SoX, HIPAA, GLBA and PCI-DSS. When these categories of data are hosted in their own data centers, the trust in systems, processes and procedures that are needed to ensure compliance rest with the employees and management of the enterprise. However when this data is resident in cloud provider infrastructure, the trusted has to be shifted to the employees and management of the cloud provider.

Hence the cloud provider has to perform the following:

IAC-F8: The IaaS cloud provider should create trust in the cloud subscriber with respect to personnel and procedures for secure operation of its infrastructure.

In order to provide this trust, the cloud provider should have the following policy in place:
IAC-SP8: The cloud provider should have a process in place to perform minimal background verification of the personnel that will be managing its cloud service related assets and resources. Also it should have in place processes and procedures for Administrator accountability (through granular logging mechanisms), Incident Notification, Response and Remediation.

6. FEATURES & POLICIES RELATING TO SUBSCRIPTION HANDLING

All of the administrative capabilities and the governing policies we have looked at so far are purely internal to the IaaS cloud provider. Let us now look at the features and associated security policies that are part of the cloud provider's service offering and hence subscriber-facing.

Every cloud provider provides a web based interface for registration of new/potential cloud subscribers.
CSR-F1: Before a new subscriber is enrolled in the service, the IaaS cloud provider should perform the following: Before a new user is formally registered and allowed to open accounts, the cloud provider should have a mechanism to perform some minimal background checks (e.g., credit history check). The threat due to a rogue subscriber is real and the "Abuse and Nefarious Use of Cloud Computing" as a threat is outlined in a study by Cloud Security Alliance [7].

In order that the cloud provider's integrity of operations is not threatened due to a rogue subscriber, the following policy is called for:
CSR-SP1: The cloud provider should perform some minimal background check on every new subscriber. Additionally there should be a means of monitoring a subscriber's network traffic to ensure that a rogue subscriber is not using the cloud provider's computing, storage and network resources to host malicious programs such as botnets, Trojan horses etc.

7. FEATURES & POLICIES RELATING TO VIRTUAL MACHINE CREATION AND OPERATION

Recall that the IaaS cloud provider provides network, computing and storage resources. The unit of computing resources that the cloud provider provides to a cloud subscriber is the Virtual Machine. Baseline features in VM resource offering by an IaaS cloud provider includes the ability for the subscriber to specify the O/S and the applications to be run on the subscribed VM and the capability to launch that VM with the required profile and subsequently stop, monitor and re-start that VM. The following is a set of features and associated policies related to VM creation and operation.

7.1 Authenticity of VM Images

CSR-F2: The cloud provider offers pre-defined VM Images or Templates. These templates may contain just a O/S (e.g., with a hardened version of O/S) or they may be application-specific (e.g., a webserver with a Linux O/S and Apache Web Server).

The security policy that will provide the authenticity of the image is as follows:
CSR-SP2: *All VM Images offered by cloud provider should be digitally signed objects so as to provide assurance to the cloud subscriber that they were created by the cloud provider or its authorized agent and have not been tampered with.*

7.2. Security Assurance for VM Images
CSR-F3: *The cloud provider would like to offer secure VM Images. A secure VM Image [8] contains in addition to the O/S and/or necessary application, all security tools typically found in a physical server such as Firewall, IDS/IPS, Anti-Malware [9], Anti-Virus along with applicable patches for the version of O/S.*

The policy that will enable this service feature is:
CSR-SP3: *The IaaS cloud service provider should define and publish baseline security configurations that it has used for creating all types of VM images it offers.*

7.3. Launching Customized VM Images
CSR-F4: *The cloud provider offers tools to customize a VM Image from a pre-defined Image or tools to build a customized VM Image from scratch.*
CSR-F5: *The cloud provider offers tools for the subscriber to launch either a pre-defined VM Image or a customized VM Image (called as Public Image and Private Image respectively by some Cloud providers). Once launched, a VM Image becomes a VM instance. Generally it will be possible to launch multiple instances using a particular VM Image (pre-defined or customized).*

An associated policy is:
CSR-SP4/5: *For all VMs launched in the cloud provider infrastructure, a unique ID should be provided. This unique ID is necessary to monitor the security status [10], [11] (as well as performance) of the VM instance. Further, the cloud provider should provide a secure channel (e.g., Virtual Private Network (VPN)) to communicate and perform all tasks (both user-level and administrative) on those VM instances.*

7.4 Design of VM Profiles and allocation of VMs to minimize impact of Denial of Service Attacks
CSR-F6: *To enable cloud subscribers to build a VM that meets their application needs, cloud providers provides a pre-defined types of VMs with designated resource profiles. A resource profile is some combination of CPU and Memory resources that will be available to the VM instance that is going to be launched and hence is an indicator of the type of performance that can be expected. For example if the subscriber needs a VM for a compute-intensive application, he/she may choose VM type whose profile has a relatively higher CPU resource as opposed to Memory resource. On the other hand if the subscriber is going to deploy the VM instance for voluminous data crunching such as database processing, he/she may choose a VM type with a profile with relatively large memory resource compared to CPU resource so as to support the large throughput.*
The associated policy is:
CSR-SP6: *The cloud provider should have VM deployment/allocation policies that assign the type of VMs that should be run on various virtualized hosts based on the resource capacity of the latter. This policy is needed to minimize the impact of any Denial of Service attack launched from any VM from incapacitating the entire physical host on which the VM resides.*

7.5 Re-starting of Dormant VMs
CSR-F7: *The IaaS cloud provider provides the capability to pause/suspend and later on re-start VMs for the cloud subscriber.*
The policy that should govern this operation is:
CSR-SP7: *The cloud provider should have a tool to enable the cloud subscriber to do the following: (a) Verify that the dormant VM being re-started conforms to a security baseline and (b) Has the ability to generate an alert with the exact violation (e.g., security patch for Guest O/S is out of date)*

The above policy is critical because of the following reasons:
1. If the VM has been dormant for a long time, the security patch for the O/S and or an application (e.g., Web server or DBMS) would have gone out of date
2. The rules for the Virtual Firewall in the VM would have to be changed following re-configuration of Virtual LANs

We are aware of the fact that some IaaS cloud service providers do not want to take responsibility for VM instances launched by cloud subscribers and they make it part of their SLAs. However, we feel that ensuring that VM instances running in your infrastructure has some minimal security is important since there is the possibility of coexistence of VMs from two different cloud subscribers on the same physical host and the threat of inter-VM attacks due to the VM from one of the subscribers being a rogue (or a victim being used as a launch pad for originating an attack).

7.6 Publication of VM Representation formats
Cloud subscribers would like to migrate their VM instances from one cloud provider to another and from their own internal infrastructure to that of a cloud provider.

To enable this, the cloud provider should provide the following:
CSR-F8: *The cloud provider provides information about the formats used for representation of VM Images*.
The following policy should go with the above feature.
CSR-SP8: *Cloud providers should publish the representational formats for the VMs running in their Virtualized infrastructure. The representational formats may vary with the type of virtualization product (technology) used by the cloud provider. The representational formats could be one of the following:*
- *Proprietary Format*
- *Open and Interoperable Format (e.g., OVF)*
- *Open and Interoperable Format with some extensions*

It may be argued that publication of the representational format for the VM images that run in the cloud provider infrastructure has a bearing on portability and interoperability of VMs and has nothing to do with the security. However, we feel that for VMs to operate with the same security protection, it is necessary for cloud providers to publish the representational format for VMs.

7.7 Migrating a VM from one Physical Host to Another
Many IaaS cloud providers would like to create the concept of clusters (groups of physical hosts) for better management of virtual machines and for efficient utilization of resources within their data center. With the help of clusters, the cloud provider can move virtual machines across the physical hosts in case of failures or planned maintenance of those hosts. Also the

migration of VMs can be used in situations where workloads need to be balanced across physical host systems.

The description of the service and its associated policies are:
CSR-F9: *The cloud provider has tools and capabilities to migrate VMs across (virtualized) physical hosts within a cluster in its infrastructure*
CSR-SP9: *IaaS cloud providers with capabilities to migrate VMs across physical hosts should have policies for the following: (a) The integrity of the VM is not jeopardized during the migration (e.g., through tampering of VM-related files-containing configuration & storage details) and*
(b) The security policy data associated with VM is also migrated (e.g., the sensitivity level of the VLAN in which the VM can be connected).

7.8 Porting Applications out of a VM or De-provisioning a VM

Cloud subscribers may port an application running in a cloud provider VM to their own internal infrastructure or to another VM in another cloud provider. Similarly they could de-provision an entire VM instance. In these instances, it is possible that the ported application is a mission critical one that has a bearing on the business competitiveness or safety of the cloud subscriber organization. Alternately, the data handled by the ported application may have privacy implication. Hence it is necessary from a security perspective that the cloud provider has well articulated policies for destruction of files related to the ported application and the data associated with it. (Even if the application files and data are moved instead of being copied, copies of files relating to application and data may still be residing in the backup volumes of the cloud service provider).

CSR-F10: *The cloud provider provides the capability for the subscriber to de-provision VMs*
CSR-SP10: *The cloud provider has a clear set of procedures for:*

- *destruction of system files (O/S and Configuration) relating to de-provisioned VMs*
- *destruction of files relating to applications ported out of the cloud provider infrastructure*

8. FEATURES AND POLICIES RELATING TO SUBSCRIBER APPLICATION-LEVEL PROTECTION

A cloud subscriber to an IaaS cloud service may install and run several applications on the set of VMs that he/she has created in the provider's infrastructure. The subscriber may demand separation of the traffic between the applications based on the following logic:

- Separation of traffic between different tiers of the application. In this scenario, the subscriber will dedicate separate VMs for each tier of the application such as Web Server, Application Server, Database Server etc.
- Separation of traffic between different environments. In this scenario, the subscriber needs logical separation of traffic between VMs belonging to different application environment entities such as Production, Development, Quality Assurance etc.
- Separation of traffic between applications with different sensitivity levels. In this scenario, the subscriber needs separation of traffic between VMs running applications of different sensitivity levels (e.g., an application processing credit card numbers Vs an application that provides access to product documentation)

In addition to separation of traffic pertaining to subscriber application, the cloud provider may need to create a separate virtual sub network for traffic relating to management of physical (virtualized) host as well as for access to storage resources under a Storage Area Network (SAN) or any other Network Attached Storage (NAS).

To enable the above the cloud provider may provide the following feature:
CSR-F11: *The cloud provider may provide capabilities to segment one physical LAN into a number of logical LANs or Virtual LANs (VLANs) to provide for separation of traffic emanating from different VMs on the same physical host [13].*
The following policy should be in place for cloud providers offering this VLAN segmentation feature.
CSR-SP11: *The policies for VLAN segmentation should consist of the following: (a) VLANs should be configured such that there is separation of traffic relating to provider's infrastructure related functions and subscriber application functions. The provider's infrastructure related functions include management of (virtualized) physical host and access to network attached storage resources (b) The configuration of virtual subnets relating to subscriber application functions should conform to the logical separation required by subscribers (based on application tiers, application sensitivity levels, application environments (production, development) etc)*

In many cloud provider infrastructures, VLAN segmentation can span several physical (virtualized hosts) whenever there exists the concept of cluster containing groups of virtualized hosts. The same policies stated above should apply to that scenario as well.

In some instances, the cloud provider can enable segmentation of traffic within a virtualized host using the following feature:
CSR-F12: *A cloud provider may install and run a virtual security appliance that runs in a specialized security-hardened VM and provides firewall (and in some instance IDS/IPS) functions.*
The following policies should be in place for offering this security appliance feature.
CSR-SP12: *The security appliance configuration policy should consist of the following: (a) Security Appliance should have visibility into traffic emanating from all VMs in the physical host. (b) The Security Appliance's firewall should be configured to restrict inter-VM traffic based on the requirements of the cloud subscriber.*

8.1 Features and Policies Relating to Service Management API

Cloud provider provides Interfaces and APIs to cloud subscribers for performing several operations. Since the cloud subscriber may be hosting several applications on the VMs, he/she may need to provision several types of information needed for application services such as authentication and authorization.

The following are some features relating to these functions:
CSR-F13: *The cloud provider provides API for the following functions:*

- *Uploading Authentication Credentials*

- *Provisioning of User Information (e.g., Account Names and Privileges)*

The security policy related to this API offering is:

CSR-SP13: The cloud provider should ensure that the interfaces and APIs they provide to cloud subscribers can only be used for the intended functions and cannot be used to launch attacks (including Denial of Service (DOS)) on the cloud provider infrastructure.

9. FEATURES AND POLICIES RELATING TO SUBSCRIBER MONITORING/MANAGEMENT CAPABILITIES

9.1 Subscriber Monitoring & Limited Management

As part of IaaS cloud offering, cloud providers provide monitoring (performance, security, usage etc) and some limited management capabilities to the cloud subscribers.

The capability relating to this service feature is described as follows:

CSR-F14: The Cloud provider may have installed several management tools for the virtualized infrastructure (individual virtualized hosts and cluster of hosts) for monitoring (performance and security states), metering the usage of resources and may provide access to some of these tools to the cloud subscribers.

The due diligence policy associated with the above is as follows:

CSR-SP14: The cloud provider should ensure that all management interfaces to hypervisor and other components of the virtualized infrastructure are connected to a dedicated VLAN meant only for management function and no other form of user interaction. Further access to the management capabilities must be provided to subscribers and cloud provider only through a mechanism that provides strong authentication (preferably multi-factor) and a robust role-based authorization.

9.2 Routing of Security Alerts

The provider capability and the associated configuration policy are listed below:

CSR-F15: Cloud provider has installed several security tools such as IDS/IPS, Malware and Virus detectors either on individual VMs or in a security appliances residing in a security-hardened VM on the host.

CSR-SP15: Security Alerts generated by the security monitoring tools should be automatically directed to the concerned subscriber. To enable implementation of this policy, the cloud provider should be able to generate a unique ID for each VM that a subscriber has launched and being able to associate that unique ID with the name and contact information for the subscriber.

10. CONCLUSIONS AND BENEFITS

In this paper, we have provided a comprehensive set of policies needed for secure operation of a virtualized infrastructure owned by a public Iaas Cloud provider. We looked at the typical set of service features offered by most IaaS cloud providers and derived security policies associated with each them based on the current state of virtualization technologies available to implement those features. The catalog of security policies derived in this paper can be of benefit to both an IaaS cloud provider and an IaaS cloud subscriber in the following ways:

- The cloud subscriber may look at the set of features advertised by the IaaS cloud provider in its service package and then verify whether the associated security policies can be adhered to by the provider.
- The IaaS cloud provider can extract the generic security policies enumerated in this paper for various administrative and subscriber-facing functions and customize it for its own infrastructure and service package.

11. REFERENCES

[1] P.Mell, T.Grance, "A NIST Definition of Cloud Computing, NIST SP 800-145, **http://csrc.nist.gov/publications/PubsDrafts.html#SP-800-145**

[2] P.Barham et al., "Xen and the Art of Virtualization,", **Proc. 19th ACM Symp. Operating System Principles**, ACM Press, 2003, pp. 164-177.

[3] R.Ghosh et al., "Performability Analysis for Infrastructure-as-a-service cloud: an interacting stochastic model approach," in **IBM Research Report, RC 25006**, 2010.

[4] D.Binning, "Top Five Cloud Computing Security Issues, **Computer Weekly**, April 2009, **http://www.computerweekly.com/Articles/2010/01/12/235782/Top-five-cloud-computing-security-issues.htm**

[5] T.Ormandy, "An Empirical study into the Security Exposure to Hosts of Hostile Virtualized Environments", 2007, **http://taviso.decsystem.org/virtsec.pdf**

[6] S. Lowe, **Mastering VMware vSphere 4**. Wiley Publishing Inc, 2009

[7] Top Threats to Cloud Computing V 1.0, Cloud Security Alliance, March 2010, **http://www.cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf**

[8] J. Wei et al., "Managing Security of Virtual Machine Images in a Cloud Environment," Proc. **ACM Cloud Computing Security Workshop**, Nov 2009, Chicago, IL, USA.

[9] S.King et al., "Implementing Malware with Virtual Machines," **Proc. IEEE Symposium on Security and Privacy**, Berkeley, CA, USA, May 2006.

[10] M. Jensen et al., "Technical security issues in cloud computing," **Proc. IEEE International Conference on Cloud computing**, Bangalore, India, Sept 21-25, 2009.

[11] B.R.Kandukuri et al., "Cloud Security Issues," **Proc. IEEE International Conference on Cloud computing**, Bangalore, India, Sept 21-25, 2009.

[12] Open Virtualization Format Specification – v 1.1.0, DMTF, January 2010, **http://www.dmtf.org/sites/default/files/standards/documents/DSP0243_1.1.0.pdf**

[13] A. Bowcom, " New Directions in Virtualization Security: How Segmentation Can Strengthen Your Security Posture" **http://www2.reflexsystems.com/l/19/ns-Virtualization-Security-pdf/JIA0J**

[14] A. Antonopoulos, J. Burke, "Practicing Virtual Security", **http://www2.reflexsystems.com/l/19/tualization-Best-Practices-pdf/ID401**