International Journal For Technological Research In Engineering
Vol. 1, Issue. 2, Oct – 2013 *ISSN (Online): 2347 - 4718*

INCORPORATING SECURITY MEASURES IN CLOUD COMPUTING USE CASES

Muneshwara M.S[1], Arvind Tejas Chandarl[2], Anil G.N.[3], Gireesh Babu C.N.[4], Mohammed Salauddin Iqbal[5]
[1, 3, 5]Department of CSE, BMS Institute of Technology, Avalahalli, Yelahanka, Bengaluru-560064.
[2]Department of CSE, S J C Institute of Technology, Chickaballapura-562101.
[4]Department of CSE, AMC Engineering College, Bengaluru-560083.

Abstract: Cloud computing has evolved from virtualization, utility computing and client-server architectures and is an extension of service oriented architectures. It has been referred to as a disruptive technology which has implications on a host of issues such as licensing, scalability, cost/performance measures, privacy and security. This paper explores some of these and the changes required in cloud computing use case scenarios to address the security issues that crop up when deploying the applications on the Internet. When end-users communicate with the Cloud while the Whole World Out There (WWOT) is an intermediary, threats can appear from a host of sources. We propose to classify them and to incorporate the responses to them in the use-case scenarios.

Keywords: **Virtualization, computer architectures, use-cases, security in cloud computing.**

I. DEVELOPING SOFTWARE FOR THE CLOUD

The US government's National Institute of Standards and Technology defines cloud computing as is a model for enabling 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. It also defines three delivery models of Software-as-a-Service (**SaaS**), Platform-as-a-service (**PaaS**) and Infrastructure-as-a-service (IaaS). It defines four deployment models which are private cloud, public cloud, community cloud and hybrid cloud. We assume that the reader is familiar with the terminologies and characterization of cloud services.

Writing software for cloud applications involves specifying the architecture and modeling the software apart from designing code. The IEEE 1471, which is a standard for architecture description of software-intensive systems, can be extended to describe the architecture of a cloud-based application. Architectures are described by a view which is basically a depiction of the components and their relationships with each other and the environment. There are various Viewpoints of the different stakeholders in the system. Architecture description languages (ADL) have evolved as a result of efforts to standardize communication among system architects. Software is now better understood through development models, such as the RUP (Rational Unified Process), and is Modeled using languages such as UML (Unified Modeling Language). Using these languages we can describe the software through structure diagrams (Class, Component, Object etc.) and Behavior diagrams (Activity, Use-Case etc.).

Cloud computing software running on server-side and on web-browsers can be modeled exactly the same way as are traditional software systems. As an illustration, Interaction diagram would still denote the interaction of the user and the system but with higher delays which come to the fore in the timing diagrams. The call to the methods of individual objects would be triggered from the web-browser at the user end.

II. APPLICATIONS RUNNING ON THE CLOUD

Applications running on the cloud run at the client facing Front-end and server back-end. Front-end software is usually a web browser with which a user interacts. The back-end consists of many servers and data storage systems. These are managed by a cloud OS called the middleware which monitors traffic and administers the system. Examples of middleware are Google Apps Engine and amazon EC2/S3. Application programming Interfaces (APIs) and system provisioning for acquisition of storage and computing power are essential for applications to run on clouds.

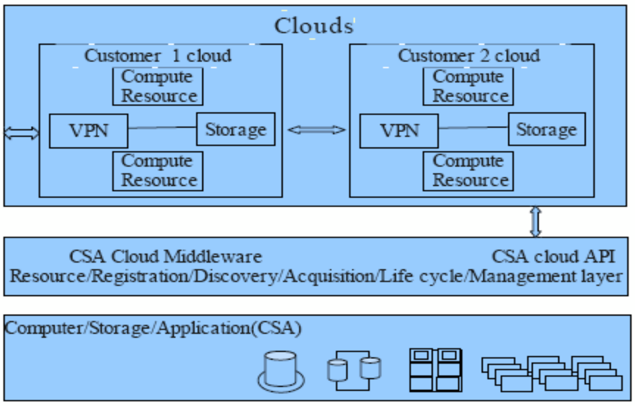

Figure 1: High Level Cloud Middleware Example

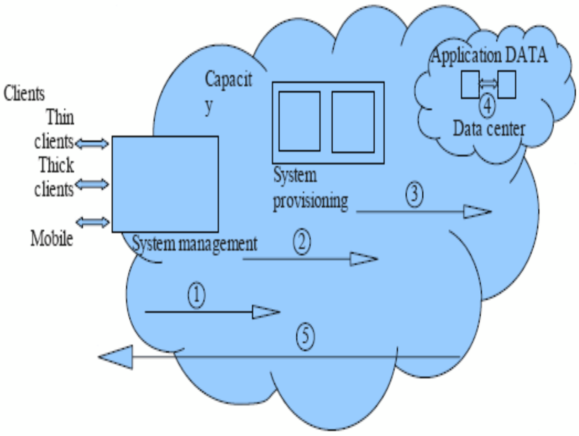

Figure 2: Cloud Computing Workflow

All applications that run on a PC also can run on the cloud. Clients will be able to access the cloud and its services from any computer linked to the Internet. Traditionally companies have been buying software (as many licenses for as many employees) and hardware. With cloud-based approach the company can pay a pay-per-use fee to a service provider. Hardware costs are reduced as system configurations need not be upgraded. Clients need to invest in a bare bones computer capable of accessing the server. Clients can send complex computational tasks to the cloud, hardware for which he may not be able to buy himself or a task which may take a lot of time on his individual system.

Clients have to store their data on private party servers and security and privacy issues arise in such a context. Security threats to the cloud computing system are of two kinds *viz* Information Security threats and Network Security threats.

III. TOP INFORMATION SECURITY THREATS IN CLOUD COMPUTING

Information security threats can be ranked according to severity although this is not done here. The following are some information security threats. [5]

Abuse and Nefarious use of Cloud Computing

Cloud computing service providers register their clients on-line without much of any background check. Anyone with a credit card can access the platform and launch his code. This has led to problems for service providers such as Paas and IaaS. Spammers and criminals have their code running on clouds and it is virtually impossible to know whether the code running on clouds is malicious or not. Remedial actions include monitoring of client network traffic and stricter registration.

Insecure Interfaces and APIs

Cloud computing servers expose a set of interfaces and APIs that enterprise and end users make use of to build software. These interfaces must be designed to prevent accidental and malicious attempts to circumvent policy. Examples of threats include unencrypted transmissions of data, improper authorizations, anonymous access and reusable passwords/tokens. Remedial actions include analyzing the service provider's security model, analyzing unknown API dependencies, ensuring strong authentication and encryption of all content.

Malicious Insiders

A malicious insider, even though is a remote possibility and any such instance has not come up as yet, is still a threat against which the service provider should keep an eye out for. Hiring policies of cloud employees and standards leave much to the discretion of the recruiter. Hobbyist hackers, criminals, corporate espionage and even nation-state sponsored intrusion are all eventualities to be guarded against. Remedial actions include laying down security breach notification procedures, transparency in information security and management practices and compliance reporting and specifying human resource policies as part of legal contracts.

Shared Technology Issues

The IaaS servers and the associated storage were not designed for sharing resources among multiple applications running on them. There is a hypervisor which mediates access between guest operating systems and physical server resources. There have been instances when guest operating systems have been able to gain inappropriate levels of control or influence on the platform. We can ameliorate this problem by conducting configuration audits and vulnerability scanning.

Data Loss or Leakages

Loosing an encoding key will render data useless, as will making changes without taking a backup. Unauthorized access to sensitive data must be prevented. Insufficient Authorization, Authentication and Audit (AAA) controls and loosing encryption and software keys are some examples. Before a user gets access to data, authentication using HMAC-SHA1 signature of the request using the user's private key is a must. Ensuring Data Integrity and Control over Data is a must in such a scenario.

Account or Service Hijacking

Exploitation of software vulnerabilities, phishing and fraud can all compromise a user account. Reusing credentials and passwords is a glaring mistake which hackers make use of. Steps can be taken to mitigate this risk by prohibiting sharing of credentials among users and passwords among services by a single user. Employing strong two-factor authentication can help here. We can also employ proactive monitoring to detect fraud.

IV. NETWORK SECURITY THREATS CLASSIFICATION

Security measures are needed to protect data going through the network between end user and cloud and between cloud servers. [2]

Distributed Denial of Service (DDOS) Attacks

In a DDOS attack servers and networks are brought down by huge amount of network traffic and users are denied access to certain Internet based service. Hackers use Botnets to perform DDOS. Botnets are a network of compromised systems on the net which participate in the attack. Subscribers and Service providers face blackmails in order to stop the attack. Service providers such as amazon have developed proprietary DDOS mitigation techniques. Man in the middle Attack

This attack uses eavesdropping on the conversations between victims. The hacker initiates conversations between two victims and relays messages between them, making them believe that they are talking directly to each other over a private connection when in fact the entire conversation is controlled by the attacker. The solution is to provide APIs via SSL protected endpoints which provide server authentication.

IP Spoofing

Spoofing is to synthesize TCP/IP packets using somebody else's IP address. The intruder gains access to the computer by sending messages to a computer with an IP address indicating that the messages are coming from a trusted source. Client softwares running on servers such as Amazon EC2 instances cannot send spoofed network traffic. The Amazon-controlled, host-based firewall infrastructure will not permit an instance to send traffic with a source IP or MAC address other than its own.

Port Scanning

An Internet user configures his computer to receive packets from a specific source to a specific port in-order to access a server. This makes the computer vulnerable to port scans. Software's running on a cloud can be disabled from port scanning the client machines. Port scans by Amazon Elastic Compute Cloud (EC2) customers are a violation of the Amazon EC2 Acceptable use Policy (AUP). Violations of the AUP are taken seriously, and every reported violation is investigated. Customers can report suspected abuse. When port scanning is detected it is stopped and blocked. Port scans of Amazon EC2 instances are generally ineffective because, by default, all inbound ports on Amazon EC2 instances are closed and are only opened by the customer.

V. SECURITY ISSUES

They are more complex in a virtualized environment because you now have to keep track of security on two tiers: the physical host security and the virtual machine security. If the physical host server's security becomes compromised, all of the virtual machines residing on that particular host server are impacted. And a compromised virtual machine might also wreak havoc on the physical host server, which may then have an ill effect on all of the other virtual machines running on that same host.

Instance Isolation: Isolation ensuring that different instances running on the same physical machine are isolated from each other. Virtualization efficiencies in the cloud require virtual machines from multiple organizations to be co- located on the same physical resources. Although traditional data center security still applies in the cloud environment, physical segregation and hardware-based security cannot protect against attacks between virtual machines on the same server. Administrative access is through the Internet rather than the controlled and restricted direct or on-premises connection that is adhered to in the traditional data center model. This increase risk of exposure will require stringent monitoring for changes in system control and access control restriction. Different instances running on the same physical machine are isolated from each other via Xen hypervisor. Amazon is active in the Xen community, which ensures awareness of the latest developments. In addition, the AWS firewalls reside within the hypervisor layer, between the physical network interface and the instance's virtual interface. All packets must pass through this layer, thus an instance's neighbors have no more access to that instance than any other host in the Internet and can be treated as if they are on separate physical hosts. The physical RAM is separated using similar mechanisms.

Host Operating System

Administrators with a business need to access the management plans are required to use Multi-factor authentication to gain access to purpose-built administration hosts. These administrative hosts are systems that are specifically designed, built, configured, and hardened to protect the management plane of the cloud. All such access is logged and audited. When an employee no longer has a business need to access the management plane, the privileges and access to those hosts and relevant systems are revoked.

Guest Operating System

Virtual instances are completely controlled by the customer. Customers have full root access or administrative control over accounts, services, and applications. AWS does not have any access rights to customer instances and cannot log into the guest OS. AWS recommends a base set of security best practices including: customer should disable password-based access to their hosts, and utilize some form of multi-factor authentication to gain access to their instances, or at a minimum certificate- based SSH Version 2 access. Additionally, customers should employ a privilege escalation mechanism with logging on a per-user basis. For example, if the guest OS is Linux, after hardening their instance, they should utilize certificate-based SSHv2 to access the virtual instance, disable remote root login, use command-line logging, and use 'sodu' for privilege escalation. Customers should generate their own key pairs in order to guarantee that they are unique, and not shared with other customers or with AWS. AWS Multi-Factor Authentication (AWS MFA) is an additional layer of security that offers enhanced control over AWS account settings. It requires a valid six-digit, single- use code from an authentication device in your physical possession in addition to your standard AWS account credentials before access is granted to an AWS account settings. This is called Multi-Factor Authentication because two factors are checked before access is granted to your account: customer need to provide both their Amazon email-id and password (the first "factor": something you know) AND the precise code from customer authentication device (the second "factor": something you have).

VI. SECURITY IN CLOUD COMPUTING USE-CASE SCENARIOS

The Enterprise Cloud Usage scenarios are intended to illustrate the most typical cloud use cases and are not meant to be an exhaustive list of realizations within a cloud environment.

Scenario 1: End User to Cloud

In this scenario, an end user is accessing data or applications in the cloud. Common applications of this type include: Email hosting, social networking sites etc. A user of Gmail logs in to Gmail portal, accesses the application and their data through any browser on any device. The user doesn't want to keep anything apart from his password, this data is stored and managed in the cloud. Most importantly, the user has no idea how the underlying architecture works. If they can get to the Internet, they can get to their data.

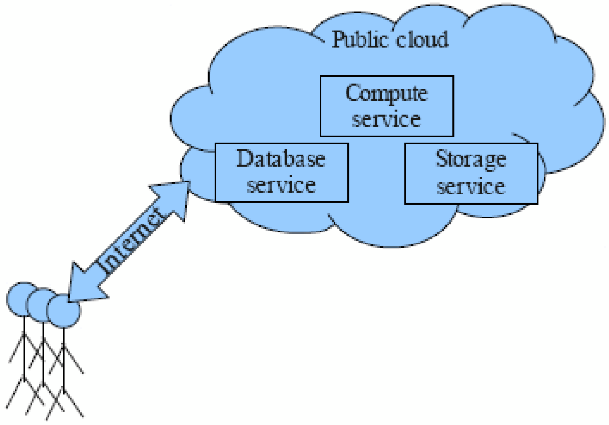

Figure 3: End user to cloud

Requirements specification

Identity: The cloud service must authenticate the end user.
An open client: Access to the cloud service should not require a particular platform or technology.
Security: Security (including privacy) is a common requirement to all use cases, although the details of those Requirements will vary widely from one use case to the next.
SLAs: Although service level agreements for end users will usually be much simpler than those for enterprises, cloud vendors must be clear about what guarantees of service they provide.

Scenario 2: Enterprise to Cloud to End User

In this scenario, an enterprise is using the cloud to deliver Data and services to the end user. When the end user interacts with the enterprise, the enterprise accesses the cloud to retrieve data and / or manipulate it, sending the results to the end user. The end user can be someone within the enterprise or an external customer

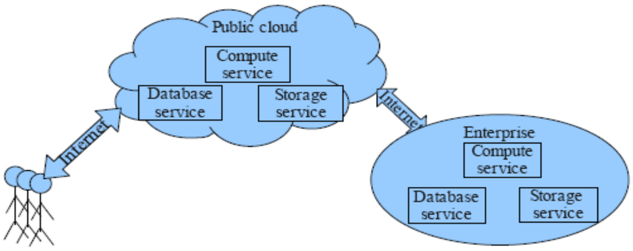

Figure 4: Enterprise to cloud to end user

Requirements Specification

Identity: The cloud service must authenticate the end user.

An open client: Access to the cloud service should not require a particular platform or technology.

Federated identity: In addition to the basic identity needed by an end user, an enterprise user is likely to have an identity with the enterprise. The ideal is that the enterprise user should have an infrastructure federating other identities that might be required by cloud services.

Location awareness: The applications cannot be moved to the cloud until cloud vendors provide an API for Determining the location of the physical hardware that delivers the cloud service.

Metering and monitoring: All cloud services must be metered and monitored for cost control, chargebacks and provisioning.

Management and Governance: Public cloud providers make it very easy to open an account and begin using cloud services; that ease of use creates the risk that individuals because of cloud services such as storage, databases and message queues is needed to track what services are used. Governance is crucial to ensure that policies and government regulations are followed wherever cloud computing is used. Other governance requirements will be industry- and geography-specific.

Security: Any use case involving an enterprise will have more sophisticated security requirements than one involving a single end user. Similarly, the more advanced enterprise use cases to follow will have equally more advanced security requirements.

A Common File Format for VMs: A VM created for one cloud vendor’s platform should be portable to another vendor’s platform. Any solution to this requirement must account for differences in the ways cloud vendors attach storage to virtual machines.

Common APIs for Cloud Storage and Middleware: The enterprise use cases require common APIs for access to cloud storage services, cloud databases, and other cloud middleware services such as message queues. Writing custom code that works only for a particular vendor’s cloud service locks the enterprise into that vendor’s system and eliminates some of the financial benefits and flexibility that cloud computing provides.

Data and Application Federation: Enterprise applications need to combine data from multiple cloud-based sources, and they need to coordinate the activities of applications running in different clouds.

SLAs and Benchmarks: In addition to the basic SLAs required by end users, enterprises who sign contracts based on SLAs will need a standard way of benchmarking performance. There must be an unambiguous way of defining what a cloud provider will deliver, and there must be an unambiguous way of measuring what was actually delivered.

Lifecycle Management: Enterprises must be able to manage the lifecycle of applications and documents. This requirement includes versioning of applications and the retention and destruction of data. Discovery is a major issue for many organizations. There are substantial legal liabilities if certain data is no longer available. In addition to data retention, in some cases an enterprise will want to make sure data is destroyed at some point.

Scenario 3: Enterprise to Cloud

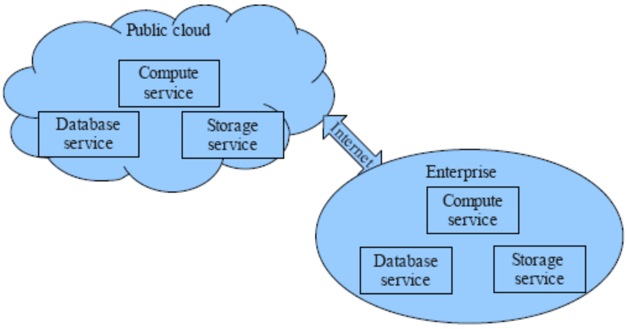

Figure 5: Enterprise to cloud

This use case involves an enterprise using cloud services for its internal processes. This might be the most common use case in the early stages of cloud computing because it gives the enterprise the most control. In this scenario, the enterprise uses cloud services to supplement the resources it needs:

Using cloud storage for backups or storage of seldom-used data

Using virtual machines in the cloud to bring additional processors online to handle peak loads.

Using applications in the cloud (SaaS) for certain enterprise functions (email, calendaring, CRM, etc.)

Using cloud databases as part of an application's processing. This could be extremely useful for sharing that database with partners, government agencies, etc.

Requirements Specification

The basic requirements of the Enterprise to Cloud use case are much the same as those for the Enterprise to Cloud to End User use case. An open client, federated identity, location awareness, metering and monitoring, management and governance, security, a common file format for VMs, common APIs for cloud storage and middleware, data and application federation, SLAs and lifecycle management all apply.

Other requirements for this use case are:

Deployment: It should be simple to build a VM image and deploy it to the cloud as necessary. When that VM image is built, it should be possible to move that image from one cloud provider to another, compensating for the different mechanisms vendors have for attaching storage to VMs. Deployment of applications to the cloud should be straightforward as well.

Industry-specific standards and protocols: Many cloud computing solutions between enterprises will use existing standards such as Rosetta Net or OAGIS. The applicable Standards will vary from one application to the next and from one industry to the next.

Scenario 4: Enterprise to Cloud to Enterprise

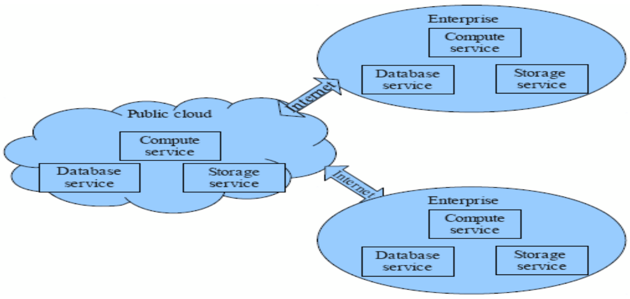

Figure 6: Enterprise to cloud to Enterprise

This use case involves two enterprises using the same cloud. The focus here is hosting resources in the cloud so that applications from the enterprises can interoperate. A supply chain is the most obvious example for this use case

Requirements Specification

The basic requirements of the Enterprise to Cloud to Enterprise use case is much the same as those for the Enterprise to Cloud use case. Identity, anope n client, federated identity, location awareness, metering and monitoring, management and governance, security, industry-specific standards, common APIs for storage and middleware, data and application federation, SLAs and lifecycle management all apply.
Other requirements for this use case are:
Transactions and concurrency: For applications and data shared by different enterprises, transactions and concurrency are vital. If two enterprises are using the same cloud-hosted application, VM, middleware or storage, it's important that any changes made by either enterprise are done reliably. **Interoperability**: Because more than one enterprise is involved, interoperability between the enterprises is essential.

Scenario 5: Private Cloud

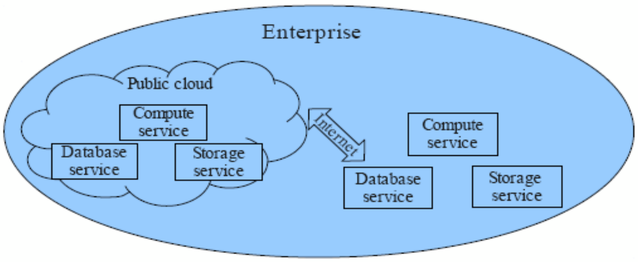

Figure 7: Private Cloud

The Private Cloud use case is different from the others in that the cloud is contained within the enterprise. This is useful for larger enterprises. For example, if the payroll department has a surge in workload on the 15th and 30th of each month, they need enough computing power to handle the maximum workload, even though their everyday workload for the rest of the month is much lower. With a private cloud, computing power is spread across the enterprise. The payroll department gets extra cycles when they need it and other departments get extra cycles when they need it. This can deliver significant savings across the enterprise.

Requirements Specification

The basic requirements of the Private Cloud use case are an open client, metering and monitoring, management and Governance, security, deployment, interoperability, a common VM format, and SLAs Note that a private cloud does not require identity, federated identity, location awareness, transactions, industry standards, common APIs for cloud middleware and lifecycle management. In many cases, consumers have to use a private cloud so that location awareness will no longer be an issue. Keeping the cloud inside the enterprise removes many of the requirements for identity management, standards and common APIs.

Scenario 6 : Changing SaaS (Software as a service) Vendors

In this scenario a cloud changes SaaS vendors. Both SaaS vendors provide the same application (CRM, accounting, word processing, etc.). Documents and data created with one vendor's software should be importable by the second vendor's software. In some cases, the customer might need to use the two vendors interchangeably.

Requirements Specification

Specific standards: Moving documents and data from one vendor’s application to another requires both applications to Support common formats. The formats involved will depend on the type of application. In some cases, standard APIs for different application types will also be required. It is important to note that there is nothing cloud-specific to these requirements. The standards for moving a document from Zoho to Google Docs are the same standards for moving a document from Microsoft Office to Open Office.

Scenario 7: Changing middleware vendors

In this scenario a cloud customer changes cloud middleware vendors. Existing data, queries, message queues and applications must be exportable from one vendor and importable by the other.

Requirements Specification

Specific standards: Moving documents and data from one vendor’s middleware to another requires both applications to support common formats.

Common APIs for Cloud Middleware: This includes all of the operations like cloud databases, cloud message queues and other middleware which require a Initiation (Creating and dropping of databases) to destroy of an APIs Connection. Cloud database vendors have enforced certain restrictions like some cloud databases do not support database schema and some do not allow joins across tables. Those restrictions are a major challenge to moving between cloud database vendors, especially for applications built on a true relational model. Other middleware services such as message queues are more similar, so finding common ground among them should be simple

Scenario 8: Changing cloud storage vendors

In this scenario a cloud customer changes cloud storage vendors.

Requirements Specification

A common API for Cloud Storage: Code that reads or writes data in one cloud storage system should work with a different system with as few changes as possible; those changes should be confined to configuration code. In a JDBC application, as an example, the format of the URL and the driver name are different for different database vendors, but the code to interact with the database is identical.

Scenario 9: Changing VM hosts

In this scenario a cloud customer wants to take virtual machines built on one cloud vendor's system and run it on Another cloud vendor's system.

Requirements specification

A common format for virtual machines: The VM format should work with any operating system. The assumption here is that the virtual machines themselves are running an operating system such as Windows or Linux. This means that the user of the virtual machine has chosen a platform prior to building a VM for the cloud, so there are no cloud-specific requirements for the software running inside the VM.

VII. CONCLUSION

The cloud computing phenomenon is generating a lot of interest worldwide because of its lower total cost of ownership, scalability, competitive differentiation, reduced complexity for customers, and faster and easier acquisition of services. While cloud offers several advantages, people come to the cloud computing topic from different points of view. Some believe that cloud to be an unsafe place. But few people find it safer than their own security provisioning, especially small businesses that do not have resources to ensure the necessary security themselves. Several large financial organizations and some government agencies are still holding back. They indicate that they will not consider moving to cloud anytime soon because they have no good way to quantify their risks. To gain total acceptance from all potential users, including individuals, small businesses to Fortune 500 firms and government, cloud computing require some standardization in the security environment and third- party certification to ensure that standards are met.

VIII. REFERENCES

[1] John Viega, McAffee, Cloud Computing and the Common Man,” published on the IEEE Journal on Cloud Computing Security, pp. 106-108, August 2009.

[2] Cloud computing: Benefits, risks and recommendations for information security, November 2009 http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment

[3] http://en.wikipedia.org/wiki/Cloud_computing.

[4] Cloud computing use cases whitepaper: a white paper produced by the cloud computing use case discussion group. 5 Aug, 2009 http://www.scribd.com/doc/17929394/Cloud-Computing-Use-Cases-Whitepaper

[5] Top Threats to cloud computing, March 2010. Cloud ComputingAlliancehttp://www.cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf

[6] Amazon web services overview of security processes http://amazonwebservices.com/pdf/AWS_Security_Whitepaper.pdf

[7] Cisco White Paper, http://www.cisco.com/en/US/ solutions/collateral/ns341/ns5 25/n s537/white_paper_ c11-532553.html, published 2009, pp. 1-6.

[8] Jon Brodkin, “Gartner: Seven Cloud-Computing Security Risks”, Available: http://www.infoworld.com, published July 2008, pp. 1-3.

[9] L. Ertaul, S. Singhal, and G. Saldamli, Cloud computing security challenges, Mathematics and Computer Science, CSU East Bay, Hayward, CA, USA, MIS, Bogazici University, Istanbul, TURKEY.