A Novel Design to Increase Trust in Cloud IaaS model

Jitendra Kumar Seth[1], **Satish Chandra**[2]

[1] *Dept of Information Technology, Ajay Kumar Garg Engineering College,*
Ghaziabad, India

[2] *Dept of Computer Science and Engineering, Jaypee Institute of Information Technology,*
Noida, India

Abstract

In IaaS services of cloud the customers demand for hardware resources as a service like memory, processor cycles, disk storage even software. IaaS services of cloud rely heavily on virtualization. The service is provided by means of virtual machine. It is not easy task for cloud users to store their valuable data over cloud because of matter of trust over cloud. Data integrity in cloud environment is ensured by the security of virtual machines. Recent survey shows the security is one of the primary concerns in adoption of cloud. In this paper a novel cloud design algorithm is proposed to ensure Virtual Machine integrity in which customer is also a part of the proposed security mechanism. The customer participation in cloud services increases customer's trust and adoption of cloud.

Keywords: *Trust, cryptography, security, integrity, IaaS, hash code.*

1. Introduction

Cloud computing is a Pay-per-Use-On-Demand model that can conveniently access shared IT resources through internet. Where the IT resources include network, server, storage, application, service and so on and they can be deployed with much quick and easy manner, and least management of and interactions with service providers [1]. Few examples of popular Cloud service providers are Microsoft Azure, Amazon EC2, and Google App Engine. Resource provisioning and flexibility are provided by means of service level agreement. During August 08/09 by IDC IT group [2], In the Cloud Computing Services Survey security, availability and performance issues still remain in the top 3 for both years the survey was done. Security is the main issue users are concerned with when considering Cloud computing solutions Cloud computing brings us the approximately infinite computing capability, good scalability, service on-demand etc. but also imposes the challenges like security, privacy, legal issues. Public cloud [3, 4] offerings are very generic and offer multi-tenancy service which all organizations might not be comfortable with. Implementing an in-house cloud is more complex to implement and are burdensome on internal resources if the organization is not large enough. Cloud service providers are continuously evolving solutions to overcome the above mentioned hurdles. Some enterprises are seeing clear benefits in shifting to the cloud and are adopting it unconditionally while some enterprises are moving non-critical applications to test the waters. Some others want to wait and watch how the technology evolves before deciding.

Interaction of consumer and consumer devices online with cloud services imposes a series of security challenges like data leakage, Virtual Machine (VM) Security, data loss and protection, data authentication, intrusion detection and resolution etc. In this paper we are resolving the issue of VM Security and producing the mutual trust between cloud vendor and customer. Virtual Machine instances can be protected by applying security countermeasures to each guest virtual machines.VM (Virtual machines) interact with each other on hardware backplane or on internet a malicious VM can affect to another targeted VM. The network level security does not detect these threats. Another security concern is with migration of VM. An attack scenario may be the migration of a malicious VM in trusted zone. VM images are prone to attack or modifications on solution is to encrypt VM all time but this approach degrades the performance of service. When a virtual machine migrated to another server it should be ensured that not a single bit is left behind the disk so that it can be recovered by other user.

The recommendations by Cloud security alliances [5] are-

1. Implementers should associate self healing capability with VM.
2. Implementers should encrypt the VM images when not in use.

3. Implementers should divide the service into categorized zones.

Cloud infrastructure [6] is multi-tenants operates on shared resources provides resource utilization but there are VMs running on same server. There is no physical separation. Therefore a malware may spread throughout the cloud. Modern attacks like root kit attacks are very difficult to be detected by traditional antivirus products. These attacks infect the key components like hypervisor and drivers that causes malicious behavior.

As more and more information on individuals and companies are placed in the cloud, concerns are beginning to grow about just how safe an environment it is. Jianfeng Yang et. al. given top most concern and issues these are security, privacy reliability, legal issues, open standards, compliance, freedom, long term viability [2]. Many businesses are putting their data on cloud data centers to improve resources utilization, speed development and deployment and reduce cost; however these new platforms are having additional avenues for threats against data, systems, network and reputation. These threats are data-stealing malware, web threats, spam, phishing, Trojans, worms, viruses, spyware, bots, and more. For most of the part all these threat are presented in the same kind of attacks. In a recent survey conduct by trend micro [7] on cloud and virtualization used by industry and business worldwide almost 45 percent are using public cloud and 46 percent are using private cloud. Inter virtual machines communications are blind to the traditional security appliances. This is said to be blind spot problem. The solution is to install a virtual machine that continuously coordinates the communication between VMs.

2. Cloud Basics

In this section some cloud basics are discussed.

2.1 Cloud Architecture

Although no clear picture of cloud architecture is meeting in literature as there are no such international standards of implementing cloud and their interoperability, the architecture is varying as per the service provider's comfortabiltity and the need of service level agreement and QoS. The essential components of cloud architecture are presented in figure 1. The cloud users are the clients who consume the services provided by cloud. Clients for the first time provide their personal and company detail and their email addresses, credit card details for billing to cloud provider to register for their cloud services. Provider then provides id and password to the consumer. Now the customer specifies their cloud service by login in their account. The SOAP request of the service is then forwarded to the cloud service provider.

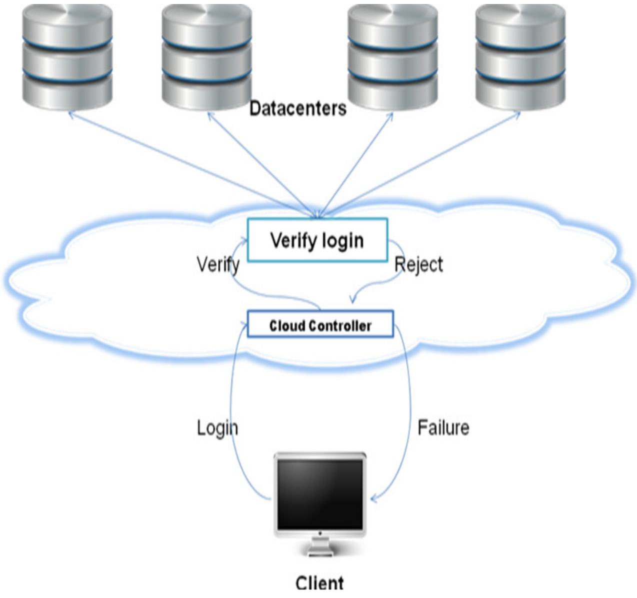


Figure 1: Basic architecture of cloud

The cloud controller accepts the request and authenticates the client for cloud service by verifying their id and password. The cloud controller can be the provider itself or some other third party. The cloud controller then checks for the host across data centers for availability of requested resource and initiate the virtual machine on host on suitable data center. Once client is connected with their VM on a host on data center the GUI of VM to client browser is loaded to interact with virtual machine. The billing of resource usage, provisioning of extra resource allocation, migration and load balancing of virtual machines and update of virtual machines all are the work of cloud controller.

The cloud architecture is segregated into following seven different layers [8]:

User Layer: In this layer cloud user's profiles are entered and processed. User profile and login are processed and maintained at cloud data center. The cloud users are provided with cloud interaction interface to interact with their user account and cloud services by means of virtual machine interface.

Virtualization Layer: users demand services are provided by configured virtual machine as per user requirement.

Service oriented module: It provide the interface to reuse the services.

Cloud module: This module is what resizes the services and tracking the usage of services charges, billing are maintained in this layer.

Cloud offering layer: This layer offers users to use value added services offered by others cloud vendors without changing underlying basic architecture.

Cloud Information layer: data structure, business case history, business intelligence and way of extracting data from database is defined in this layer.
Cloud quality and monitoring layer: This module monitor for the services upto agreed QoS.

Cloud is a cost effective platform for the business that is of medium or of small scale or to those whose budget is low or just started and establishing. Basically, virtualization reduces complexity. In that way, a virtualized network is easier to manage, hence less cost to administrating a complex solution and enhances user's friendliness. Enhanced scalability, flexibility, and utilization provide additional cost savings. Automation is an additional functionality available through virtualization. All these features are transparent to user and give a clear picture of the cloud to the user [9]. Cloud should charge only when the resources are in use and not to charge for resource once assigned to their consumers and are idle. Automatic resource provisioning and scaling supports efficient functionality of the business.

3. Cloud Security Overview

In this section a brief overview of current security threats in cloud are discussed.

The analysis of management interface are done on Amazon EC2 and S3 services, the control interfaces could be compromised via the novel signature wrapping and advanced XSS techniques. Similarly, the Eucalyptus control interfaces were vulnerable to classical signature wrapping attacks, and had nearly no protection against XSS[10].The XML signature wrapping attack by using SOAP request occurred in cloud services. Using XML signature wrapping attack the intruder can bypass the user login verification and may prove them as legitimate user. Another threat to cloud management interface is cross site script (XSS) - The first script injection vulnerability discovered on the aws.amazon.com domain was caused by a download link used to retrieve X.509 certificates issued by Amazon.

Clouds have the following types of intrusion threats [11]:

i. Insider attacks
ii. Flooding attack
iii. User to root attacks
iv. Attacks on virtual machine (VM) or hypervisor
v. Backdoor channel attacks etc.

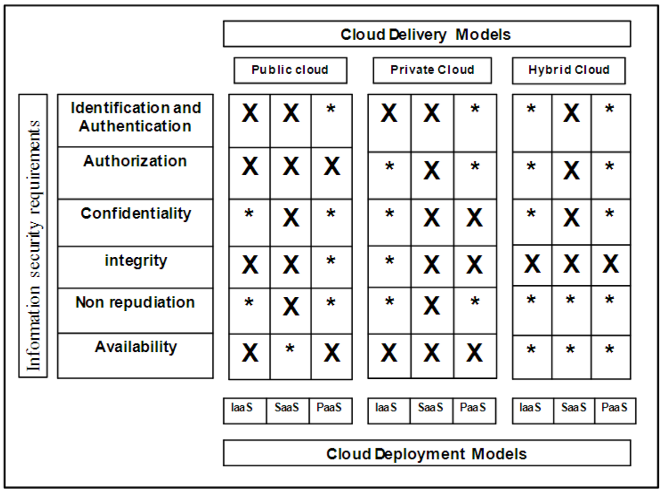
According to Gurdeep Singh et. al. [12] critical information on cloud inspires the attacker to steal and threat them hence security is one of the prime concerns of cloud. Author focuses on security of VM images which are foundation of cloud security. Today's cloud computing platforms are typically "opaque": Amazon EC2 users only receive virtual units of CPU and memory, and physical details of the platform are hidden. Such opacity prevents programs from online optimizations and deployment adjustment, and is penalizing the very applications cloud computing attempts to attract: high-performance software. On the other extreme, a completely transparent design of clouds would lead to severe security and reliability concerns. Yu David Liu et. al. had given an idea how we can customize our cloud features using given APIs. They are given two APIs, one to cloud side and another one to application side. Interface designs that can help cloud programs to fine-tune performance, and how it may impact on other important issues of cloud computing, such as security, scheduling, and pricing [13]. Concretely, they propose a new object-oriented programming language, iCloud, for cloud computing. iCloud is designed with the philosophy of Interaction-Based Programming. Here is cloud services can be abstracted as classes with connectors. Application side has a DB connector and Sch connector. This means that a MyApp object can participate in two and only two kinds of interactions with other objects at run time. Connectors serve as the complete specification of the cloud's exposure to the programmer. To avoid "too much" transparency, cloud service providers need to, and only need to, design connectors carefully. A connector-based design is a boon for security, so that access control policies are only needed on these well-defined interfaces. Each connector may have a number of imports and exports. Each export is a method the connector can provide to "the other party" (i.e. whoever is connected to this connector), and each import is a signature specifying what it expects the other party to provide. Each connector may also hold connection-specific data.

3.1 Security in cloud categories (SaaS, PaaS, IaaS)

Literature survey is being done on security in SaaS, PaaS and IaaS and is summarized as follows. Currently Cloud computing clients have to trust 3rd party cloud providers on many fronts, especially on the availability of cloud service as well as data security. Therefore the SLA forms an integral part of a client's first line of defense. The SLA thus becomes the solitary legal agreement between the service provider and client [14]. Figure 2 shows the different cloud delivery models and deployment models are matched up against the information security requirements with an "X" denoting mandatory requirements and an asterisk (*) denoting optional requirements. The only means that the cloud provider can gain the trust of clients is through the SLA; therefore the

SLA has to be standardized. The main aspects as a guideline, which the SLA contains, are:

1. Services to be delivered, performance,
2. Tracking and Reporting
3. Problem Management
4. Legal Compliance
5. Resolution of Disputes Customer Duties
6. Security responsibility
7. Confidential Information Termination.



Information security requirements	Cloud Delivery Models								
	Public cloud			Private Cloud			Hybrid Cloud		
	IaaS	SaaS	PaaS	IaaS	SaaS	PaaS	IaaS	SaaS	PaaS
Identification and Authentication	X	X	*	X	X	*	*	X	*
Authorization	X	X	X	*	X	*	*	X	*
Confidentiality	*	X	*	*	X	X	*	X	*
integrity	X	X	*	*	X	X	X	X	X
Non repudiation	*	X	*	*	X	*	*	*	*
Availability	X	*	X	X	X	X	*	*	*
	Cloud Deployment Models								

Figure 2: Cloud security requirements

Potential Cloud organizations and vendors need to be aware that it may become easier for attackers to threaten clouds by moving towards a single cloud interface. The shift to Cloud computing moved much of a user's normal activity to the Web browser. Web browsers generally store all of a user's saved passwords, browsing history and other sensitive information in a single place. As such it is possible for malicious websites to exploit browser vulnerabilities in order to steal information associated with other existing or previous browsing sessions, such as a logged in email account or online banking session. It is for this reason that some security experts recommend that consumers use one web browser for general surfing, and another for more sensitive tasks, such as online banking. Often, usernames and passwords are transmitted to remote servers via unencrypted network connections. In cases where encryption is used, it is typically only used to transmit the initial login information, while all other subsequent data is sent in the clear. This data can easily be snooped on by hackers. This exposes users to significant risks when they connect to the services using public wireless networks to any Cloud Service.

SaaS and PaaS Security issues are as follows: SaaS (Netflix, MOG, Google Apps, Box.net, Dropbox and Apple's new iCloud) typically focuses on managing access to applications, while PaaS (Google App Engine, Microsoft Azure, Saleforce's Force.com, the Salesforce-owned Heroku, and Engine Yard) focuses primarily on protecting data, and IaaS (Amazon, Microsoft, VMWare, Rackspace and Red Hat etc.) focuses on managing virtual machines.Since SaaS delivers applications from the cloud, the main risk is likely to stem from multiple passwords accessing applications [15]. "An organization can solve these issues by opting for a single sign-on option between on-premise systems and cloud. By leveraging a single sign-on option, users are able to access both their own desktops and any cloud services via a single password. This approach also reduces the incidences of dangling accounts – which are vulnerable to unauthorized usage – after users leave organizations."PaaS can be inherently secure, but the risk is slow system performance. That's because data encryption is recommended before data is sent to PaaS cloud providers. The risk is that encrypting every piece of data will also eat up consumer organizations' CPU cycles and slow things down. Still, any solution implemented should broker the connection to the cloud service and automatically encrypt "confidential user data such as home addresses, social security numbers or even medical records." Audit trails provide valuable information about how an organization's employees are interacting with specific Cloud services, legitimately or otherwise.

Lombardi et. al. [16] shows the security of cloud by protecting the integrity of guest virtual machines and cloud components. Advance cloud protection system (ACPS) effectively monitors the integrity of guest virtual machines and infrastructure and remains transparent to VMs and cloud users. Accountability produces a record of action which can be examined when something goes wrong. All modules of ACPS are located on host side. ACPS makes use of Qemu to access the guest VMs. Suspicious guest activities (e.g. system call invocation) can be noticed by the Interceptor and recorded by the Warning Recorder into the Warning Pool, where the potential threat will be evaluated by the Evaluator component. Evaluation components are evaluator and hasher is always active. Although ACPS is a host based security mechanism of virtual machine it does not involves the client to ensure their virtual machine integrity; even the client does not know their virtual machine has been compromised. In this proposed security mechanism Client is also part of their security assurance hence produces mutual trust between cloud vendor and the client. Integrity one of the three major security aspects confidentiality, integrity and availability is resolved for VMs with client involvement. VMs are stored on vendor's database as a unique file of customers. Our proposed idea detects the infections of the VM by checking integrity of theses stored files. As soon as the unauthorized modification to VM is detected at vendor side the appropriate security mechanism may run and recover from these unauthorized modifications and restores the VM in user account. The detailed idea is described in section 4.

4. Proposed Security algorithm ensures integrity of VM

In cloud computing, to register with cloud services the customers provide their personal information including e-mail and credit card information to the cloud service provider. Customers are provided with unique user id and password via their registered e-mail from the cloud service provider. By using the provided user id and password customer login the cloud service and a pair of public and private key for the customer is generated and the public key is registered with the cloud host for secure transmission between both the parties. Now customer's encrypted request (with the private key) is served by cloud host [17]. Here clients do not play any role in their security assurance. Client is totally dependent on cloud service provider's security mechanism for his / her data security, running on cloud host.

4.1 Hash Code

Hash code is a cryptographic technique to check message integrity. A hash function accept a variable size message M as input and produces a fixed size output referred to as hash code H(M).The hash code is also referred as message digest or hash value. The hash code is a function of all the bits of the message and provides error detection capability. A change to any bit or bits in the message results in a change to hash code. An important application of secure hashes is verification of message integrity. As of 2009, the two most commonly used cryptographic hash functions are MD5 and SHA-1. All well-known hash functions, including MD4, MD5, SHA-1 and SHA-2 are built from block-cipher-like components designed for the purpose, with feedback to ensure that the resulting function is not invertible.

4.2 The proposed security model

In our proposed model, after successful registration of client with the cloud provider a hash code checker module is installed at the client machine by cloud service provider, which reserves few KBs of memory in the disk for future use. This memory space is restricted and only used by hash code checker module. After successful installation of hash code checker module at client machine, cloud controller module which is a part of a provider's cloud service management software, sends a default valid hash value encrypted by cloud provider's public key to the hash code checker module at client which stores the encrypted hash in client's machine restricted memory space. Whenever a client logins to the cloud service the hash code checker appended the encrypted hash value with the login information and sent to the cloud provider. After verification of login information provider also decrypt the received hash value with his private key and compare the decrypted hash value with the stored virtual machine image hash value at provider's side if both the hash values are identical then client is successfully authenticated for cloud service. Once the virtual machine (VM) is allocated to the client and client workout on the allocated virtual machine after all the work done on VM client request for sign out, before logout confirmation to client and shutting down the virtual machine the hash value of saved up-to-date virtual machine image is computed at datacenter by using cryptographic techniques like MD5 or SHA-1 and encrypted with the cloud provider public key and transmitted encrypted hash value to the client which is received and stored in restricted memory area by the hash code checker module. Each time a client logins to the cloud service the hash code checker module appends the last saved encrypted hash value of virtual machine with the login information.

Figures 3a & 3b shows the design of the proposed security mechanism discussed above.

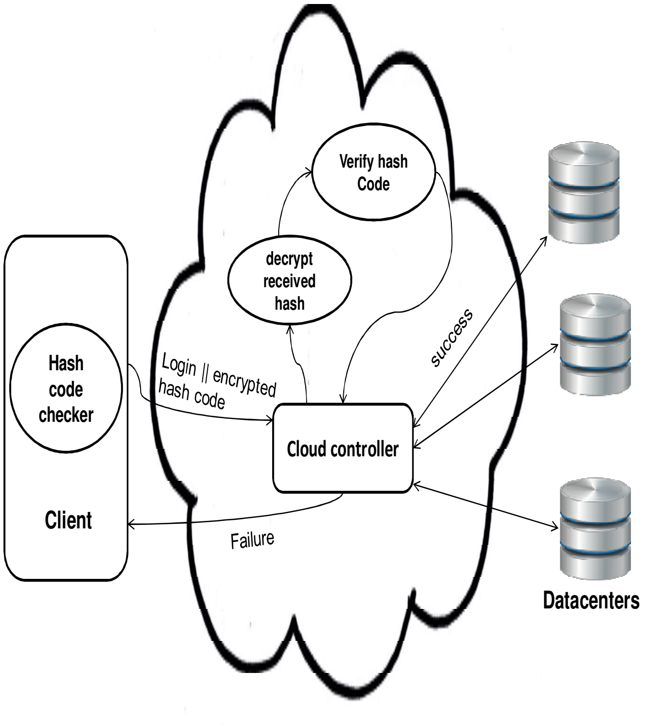


Figure 3a: Two way authentication of user by using login and hash code

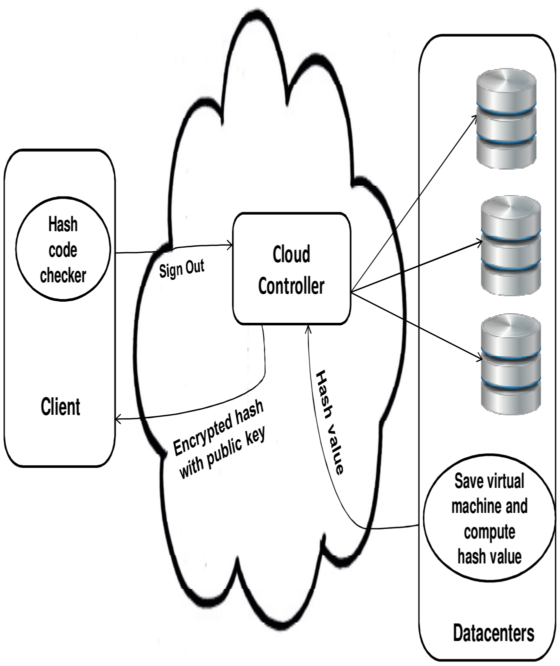

Hash code checker
Client
Sign Out
Cloud Controller
Encrypted hash with public key
Hash value
Save virtual machine and compute hash value
Datacenters

Figure 3b: Transfer of encrypted hash value to client machine after logout

4.3 Proposed Integrity check algorithm of virtual machine

The aforementioned approach can also be written in following steps:

1. Client registers with cloud service provider
2. After successful registration client is provided with user id and password.
3. Client logins and hash code checker is installed at client machine.
4. Hash code checker stores encrypted hash value to restricted memory area at client machine
5. Each time client login to cloud service the hash code checker module append encrypted hash code with login information
6. Cloud controller verify login information then decrypt received hash code by using provider's private key and compare with hash value of stored virtual machine image at data centers.
7. Once user is verified in both the ways successfully then only login is confirmed and last saved user's virtual machine image is loaded on data center and control is provided to user browser.
8. If user login fails in any of the ways then alternate mechanism addressed in section 6 points d and f executes.
9. After work out on virtual machine user signals logout
10. Cloud Provider save the virtual machine image and computes the hash value of VM image and encrypts it (by using Provider's Public Key).
11. Encrypted Hash value is sent to the Client by cloud controller.
12. Hash code checker module at client stores the received encrypted hash value and sends the acknowledgment to Cloud Provider, which then signals successful, sign-out to the Client.
13. Each time Client logins; the last saved encrypted hash value at Client is appended with login Information and all steps 6 to 12 repeated each time.

5. Experiment

In our experiment NetBeans 7.0.1 and jdk 1.6 were used with Libvirt API to interact with guest virtual machines. Qemu is used as a tool between Libvirt and Hypervisor. KVM hypervisor is used on Ubuntu 12.04. We have created Guest virtual machines from the .iso images of various Linux based operating systems like Ubuntu, Fedora, and DSL Linux etc. VM configuration is provided by using XML API of Libvirt. In our experiments we have given the configuration of VM creation as follows: one logical processor, 347 MB of RAM, and dsl linux .iso image. We have created, suspended, resume and saved virtual machines using Java. We have also computed the hash code of virtual machine using java security package [18] hash code algorithm SHA-1 and stored them in a file. Before the next boot of virtual machine the hash code of stored VM image file is again computed and compared with the stored hash value they are matched and VM is started.

The following depicts one of the output of our experiment:

```
Virtual Machine Name=mydslvm---Time of Creation:--Wed May
08 23:09:51 IST 2013
Virtual Machine Name=mydslvm---Time of Suspend:--23:11:39
Virtual Machine Name=mydslvm/nTime of Resume:--23:12:2
Virtual Machine Name=mydslvm---Time of Suspend:--23:12:24
Virtual Machine Name=mydslvm---Time of hashcode:--Wed
May 08 23:12:45 IST 2013:12:45
Hash code is -
136763718569839279811069244876589845739944818196
```

For the next boot of VM

```
Virtual Machine Name=mydslvm---Time of hashcode:--Wed
May 08 23:13:48 IST 2013:13:48
```

Hash code is -
136763718569839279811069244876589845739944818196

6. Benefits of proposed security mechanism

This approach is very much useful in following respects-

a) It produces two way authentication of client to cloud host. One with something stored at cloud host (login information) second something stored (encrypted hash value of VM) with the client machine.

b) This security approach prevents XML signature wrapping attack and script injection attack. If the signature (id, password and public or private key consumer side) is compromised [10] by such attacks even though the attacker still cannot prove their authenticity as client side hash code is encrypted by cloud providers public key and can only decrypted by providers private key.

c) It enhances the mutual trust between the cloud provider and the cloud service consumer. Client machine is also playing a crucial role in their security mechanism.

d) If the client VM is targeted and compromised by attacker and intruder, there are some unauthorized changes or modification to virtual machine at the host, hence there is a mismatch of hash values between received hash value and stored hash value on the host and client login is unsuccessful. It may also be the case with wrong password so first password is confirmed to client by using client e-mail id; if then after the login is not successful Then the strong intrusion detection mechanism by host to the targeted virtual machine is carried out and if found suspicious replaced by backup virtual machine confirm successful login to client.

e) Even if there is a problem with restoration of up-to-date virtual machine then some previous version of virtual machine integrity is ensured by client side stored hash value and client data is restored upto some recent version.

f) If client side security module, hash code checker is compromised then client login is again unsuccessful. Client is provided password by using their email id or other medium. If again unsuccessful login then a new copy of hash code checker module is installed at client machine and login password and encrypted last saved hash value at the host is provided to client security module.

7. Conclusion

From the proposed security approach it can be seen that this security scheme provides two way authentication and also prevents xml signature wrapping attack and script injection attack. It also stores hash information at client machine so increasing level of mutual trust. Client trust is produced as client is assured any intruder cannot login the Client without knowing the hash value stored at Client machine even though login information is compromised. This scheme is also helpful in data recovery process and triggers intrusion detection mechanism as found suspicious. It provides two way security in which client is also playing an important role. If recovery is not upto date then some previous version of VM can be restored with the help of stored hash value at client machine and backup VMs on host. Hence this security approach reduces the threat level to cloud and also producing the trust to those peoples worrying to adopt cloud services for their data protection.

References

[1] Junjie Peng et. al, "Comparison of Several Cloud Computing Platforms" in Second International Symposium on Information Science and Engineering, IEEE-2009.

[2] Jianfeng Yang, Zhibin Chen, "Cloud Computing Research and Security Issues" in Computational Intelligence and Software Engineering (CiSE), IEEE-2010.

[3] Kirchberg, Markus; Lee, Bu Sung," Efficient Migration of Virtual Machines between Public and Private Cloud", Cloud Computing Technology and Science (CloudCom), IEEE 2011.

[4] Simmons, Bradley; Smit, Michael; Litoiu, Marin," An architecture for overlaying private clouds on public providers", Network and service management (cnsm), 2012.

[5] Cloud security alliances, 2011.

[6] Raghu Yeluri et. al, "Building Trust and Compliance in the Cloud for Services " in Annual SRII Global Conference, IEEE 2012.

[7] Virtualization and Cloud Computing: Security Threats to Evolving Data Centers, Trend Micro, 2012

[8] Amarnath Jasti et.al. ," Security in Multi-Tenancy Cloud" in Security Technology (ICCST), 2010 IEEE.

[9] "Virtual Enterprise Model for Enabling Cloud Computing for SMMEs" in *ISWSA'11*, April 18–20, ACM 2011.

[10] Juraj Somorovsky, Mario Heiderich et.al, "All Your Clouds are Belong to us – Security Analysis of Cloud Management Interfaces" in CCSW'11 ACM-2011.

[11] Chirag Modi, "A survey of intrusion detection techniques in Cloud" in Journal of Network and Computer Applications, Elsevier 2012.

[12] Gurdeep Singh Bindra et. al, "Cloud Security: Analysis and Risk Management of VM Images", in International Conference on Information and Automation (ICIA), IEEE 2012.

[13] Yu David Liu and Kartik Gopalan. " Interaction-Based Programming Towards Translucent Clouds (Position Paper)" in APLWACA ACM-2010.

[14] Ramgovind S et. al, "The Management of Security in Cloud Computing" in Information Security for South Africa (ISSA), IEEE-2010.

[15] Joe McKendrick "SaaS, PaaS and IaaS: three cloud models; three very different risks" on ZDNet April 2012

[16] Flavio Lombardi et. al, "Secure virtualization for cloud computing" in Journal of Network and Computer Applications 2010.

[17] Sven Bugiel et. al, "AmazonIA: When Elasticity Snaps Back" in CCS'11, October 17–21, 2011, Chicago, Illinois, USA, ACM 2011.

[18] http://www.roseindia.net/java/java-security.shtml

Jitendra Kumar Seth is an Assistant professor in Information Technology Department at Ajay Kumar Garg Engineering College, Ghaziabad, India. He did his B.Tech in CSE from UPTU Lucknow and M.Tech in CSE from Shobhit University Meerut. Currently he is pursuing his PhD in CSE from Jaypee Institute of Information Technology,Noida, India.His area of interest is cloud computing.

Satish Chandra is an Assistant professor in the Department of Computer Science & Engineering at Jaypee Institute of Information Technology, Noida, India. He did his B.E. and M.Tech. from Birla Institute of Technology, Mesra, Ranchi and PhD from JUIT, Solan, India. His area of interest includes Cloud Computing, Machine Learning, Artificial Intelligence, Biologically Inspired computing and Medical Image Analysis.