ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

Protection of Cloud Users Work Environment Using Trusted Platform Module

[I]Loubna Dali, [II]Raymond Tiwang, [III]Hoda Elsayed
[I,II,III]Dept. of computer sciences, Bowie State University, USA

Abstract
Cloud computing has recently emerged into our daily life as a utility service, where customers pay only for the used resources and services. The cloud computing is becoming the next big thing in IT industry by providing a big pool of services based on virtual computing resources through the internet. These services are being executed and implemented via virtual machines. The customer can demand and release the image of virtual machine without checking whether the environment where their program runs is safe and trustworthy. In this paper we propose a trusted virtual machine in order to prevent insider attacks, using trusted nodes assigned by a trusted third party.

Keywords
Trusted Platform Module, Trusted Cloud Computing, Cloud Broker, Virtual machines.

I. Introduction

Cloud computing provides a centralized pool of configurable computing resources and mechanisms to enable services in a way similar to utility-based systems such as electricity, water but delivered over the Internet. Cloud based service has five characteristics as following: (i) On-demand self-service: A consumer can unilaterally provision computing capabilities as needed and automatically, without human interaction with a service provider. (ii) Broad network access: Computing capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g. mobile phones, laptops, and PDAs) as well as other traditional or cloud based software services. (iii) Resource pooling: A provider pools computing resources to serve several consumers using a multi-tenant model, which dynamically assigns and reassigns physical and virtual resources according to consumer demand. Having a degree of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources. (iv) Rapid elasticity: Capabilities can be rapidly and elastically provisioned, in most cases automatically, and rapidly released to quickly scale out and scale in. In the consumer side, the capabilities appear to be unlimited and can be purchased in any quantity at any time. (v) Measured service: Cloud systems automatically control and optimize resource usage by leveraging a metering capability according to the service type. The usage can be controlled, and reported, offering transparency for both the provider and the consumer.

There are four deployment models for cloud services that vary to address specific requirements according to customer needs: (i) Public Cloud: The cloud is made available to the general public or a large industry group and is owned by an organization selling cloud services. (ii) Private Cloud: The cloud is operated solely for a single organization. Being managed by the organization or by a third party, possibly having on-premises or off- premises infrastructures.

(iii) Community Cloud: The cloud is shared by several organizations to support a specific community that has shared concerns and needs. It may be managed by the organizations or by a third party and may exist on- premises or off-premises. (iv) Hybrid Cloud: The cloud infrastructure consists of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability.

In general, clouds offer services at three different levels [4]: IaaS, PaaS, and SaaS. However, some providers can expose services at multiple levels. (i) Infrastructure as a Service (IaaS): Infrastructure-as-a-Service (IaaS) involves outsourcing the basic infrastructure used to support operations including storage, hardware, servers, and networking components. The service provider owns the infrastructure equipment and is responsible for housing, running, and maintaining it. The customer typically pays on a per-use basis however uses his own platform (Windows, Unix), and applications. (ii) Platform as a Service (PaaS): involves outsourcing the basic infrastructure and platform (Windows, Unix). PaaS facilitates deploying applications without the cost and complexity of buying and managing the underlying hardware and software where the applications are hosted. Yet The customer uses their own applications.

(iii) Software as a Service (SaaS): Also referred to as "software on demand," this service model involves outsourcing the infrastructure, platform, and software/applications. Typically, these services are available to the customer for a fee, pay-as-you-go, or a no charge model.

The majority of organization has shifted its IT infrastructure to cloud computing, however, they have to be aware of the risks and threads that might occur and will cause data loss.

Being part of cloud services , IaaS overcome most of known threads, in addition to that, the IaaS Cloud Provider may provide better security than the customer existing software. Better security may come in part because it is critical for the IaaS Cloud Provider and is part of their main business, what we called the In-house security. However, the possibility of being attacked either accidentally or intentionally can still occur. (Dali et al) []. In figure 1 statistics shows that the main concern of cloud customers is neither the integrity nor the availability but they are more concerned about their confidentiality.

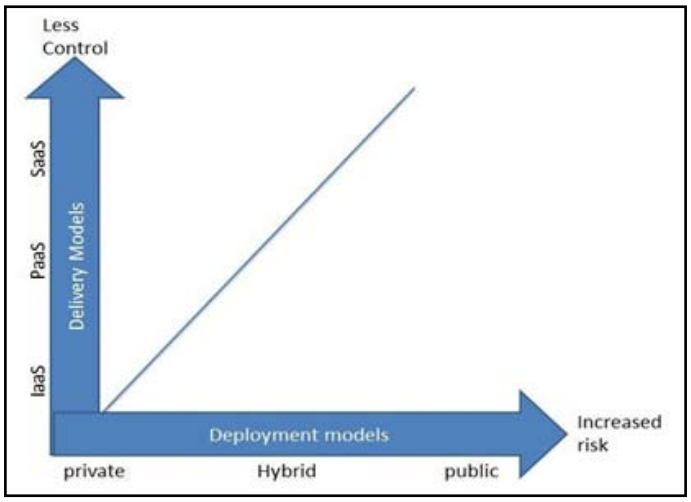

Fig.1 : Risk Relationship With IaaS Deployments Model and cloud service delivery

Focusing on external attackers, the cloud providers raise the security awareness by encrypting the data at the client side and decrypt it once received to the cloud end side. This technique will surely enhance the security of data and prevent attacks during the transfer. However,and at the decryption phase, whoever has a privileged access can affect all computer security elements and range from stealing sensitive data to injecting Trojan viruses in a system or network. Insiders also may affect system availability by overloading computer/network storage or processing capacity, that leads to system crashes so the customer data will be unavailable. As a result, the cloud customer will not be able to handle or control their own space of work (Virtual machines). This specific flaw makes the companies afraid to move their business from traditional IT environment to Cloud environment, despite all the benefits that cloud provide and all the efforts they make to gain trust by restricting access and reinforce policies and rules to decrease the risk of insiders. To resolve this issue, we propose a model that will combine the power of trusted platform module with the availability of virtual machine, also we will involve third party access security brokers. To make the virtual machine, images are stored in different trusted nodes in order to make the computation more secure.

To implement this proposal, we used CloudStack which is an open source software, considered as turnkey solution designed to deploy and manage large networks of virtual machines, as a highly available, highly scalable Infrastructure, that pools computing resources to build public, private and hybrid Infrastructure as a Service (IaaS) clouds. As seen in Figure 2 the CloudStack, has one or more Pod cluster manager who run a virtual machine monitor to host customer's virtual machine.

Its components are namely :

- Hosts: Servers onto which services will be provisioned
- Primary Storage: VM storage
- Cluster: A grouping of hosts and their associated storage
- Pod: Collection of clusters
- Secondary Storage: Template, snapshot and ISO storage
- Zone: Collection of pods, network offerings and secondary storage
- Management Server Farm: Responsible for all management and provisioning tasks

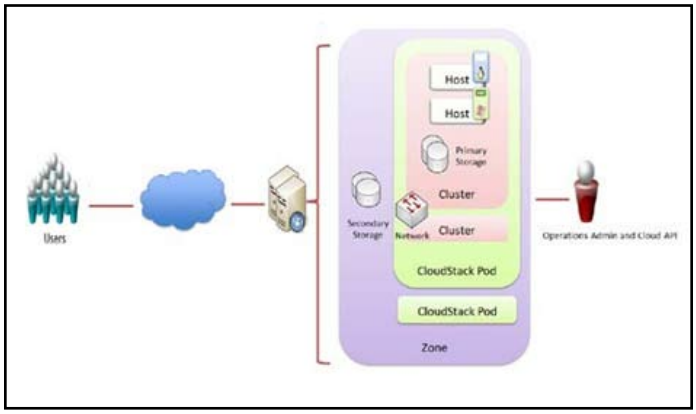

Fig. 2: CloudStack Components

The cloud customer requests IaaS service to implement its system. Yet, he remains susceptible to hardware or software vulnerability such as malicious algorithms or electromagnetic radiation. Also, in order to break the confidentiality wall, the insider who usually is administrator with privileged access, might run attacks to get to the information computed by the VMs. This information can be personal records, intellectual property or account number, the insider may also install or execute some programs in contemplation of leaking stored data or copy what was electronically transmitted to an outsider (competitor, press media or regulators). As a result, the cloud customer might face loss of assets, legal liabilities or even closing their businesses.
This phenomenon needs an immediate solution, that is establishment of trust system that build up the trust between the client and CP. So the cloud customers will run their programs within a trusted environment.
This solution is based on Trusted Platform Module in corporation with trusted third party.
Trusted Platform Module:
The Trusted Platform Machine (TPM) is used to enhance system security, by offering a way of secure storing sensitive information and allowing verification of system integrity. TPM is a hardware device that is basically a secure micro-controller with added cryptographic functionality. It works with supporting software and firmware to prevent unauthorized access. The TPM contains a hardware engine to perform up to 2048-bit RSA encryption/decryption.
The TPM uses its built-in RSA engine during digital signing and key wrapping operations. Since Cloud- based systems mainly lay on virtualization thus the extension of TPMs can be used with virtual machines (VMs) called TPM virtualization and it results in a virtual TPM (vTPM) design.
TPM offers three main benefits: storage for secure content, secure specific reports by the platform requirements, and hardware authentication. Using a TPM module for secure content, the user has the advantage of storing files securely without relying on software based operating system. In the case of mobile devices, users can encrypt the entire hard drives using TPM. Thus reducing the risk of losing sensitive data. It is possible for many users to connect to an unsecured storage device on an insecure network and protect shared information without the need for a secure common operating system using TPM 1.2 technology. For example, many users today rely on secure storage servers hosted

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

online so they can share data among multiple devices and access information everywhere. This requires the user confidence that their information hosted is set with administrators, server and client OS and additional security software, and the server BIOS and CPU.

The auditor also requires no contact with the transmitter and should only rely on the TPM chip in the original machine. Significantly, the one-time certificates cannot be forged or falsified even a hacked machine that could open their use for multiple applications offline.

A TPM can also collect, secure, and report information about the status of computer components such as the BIOS, boot records and sectors, applications and OS. The TPM can do so using the platform configuration registers (PCR) to pass safely measured by component information on the state of another component. During startup, the X component and Y component measuring status and inserts the data into a PCR where it is fixed and able to provide the state of the platform from the moment. In order to pass this information known as the configuration of the platform to another entity, the TPM encrypts the configuration using a trusted signing key that can be decrypted by a remote TPM key with the required credentials.

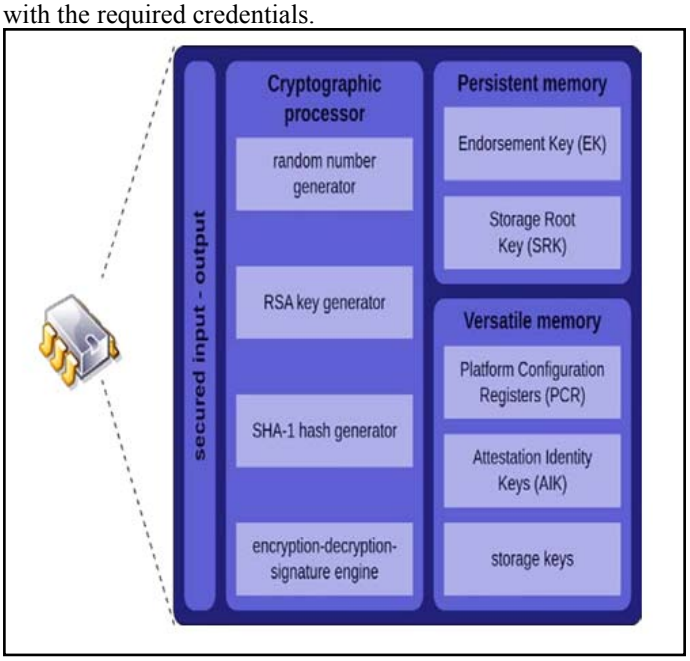

Fig. 3: Trusted Platform Module

The TPM has the following capabilities:

- performing public key cryptographic operations
- computing hash functions
- key management and generation
- secure storage of keys and other secret data
- random number generation
- integrity measurement
- attestation

The third Party :Cloud Broker

This model Inter-Cloud (see Figure 4) is characterized by indirect interconnection between two or more CSP through an entity called Inter-Cloud Service Broker (ISB). An ISB type entity provides interworking service functions between interconnected CSP and also provides brokerage service functions for one or several interconnected Cloud Service Provider as well as the Cloud Service User. In addition, the Cloud Broker (responsible for the brokerage service) has emerged as an intermediate layer between the CSP and the CSU to help the user to choose the best services in a cloud- based environment. Furthermore, the Cloud Broker can act as

a negotiator for the user with many cloud environments. Thus, it can search and book available resources in other CSP, based on different levels of service to avoid SLA violations (Service Level Agreement).

The Inter-Cloud Service Broker can provide three types of services:

- Intermediation services: with this type of service, IBS allows an improvement of the service by adding other features such as access management, identity management, performance reporting, security measures, etc.
- Aggregation Service: providing an aggregation service type, Cloud Broker offers a combination and integration of multiple services in one new service. Thus, it allows the integration of data and ensures the security of data flow between the CSU and the CSP.
- Arbitration services: with this type of service, Cloud Broker has the option to choose services from multiple cloud providers. Thus, it allows flexible and opportunistic choices. For example the Cloud Broker can use a credit score service to well select a source within the best score.

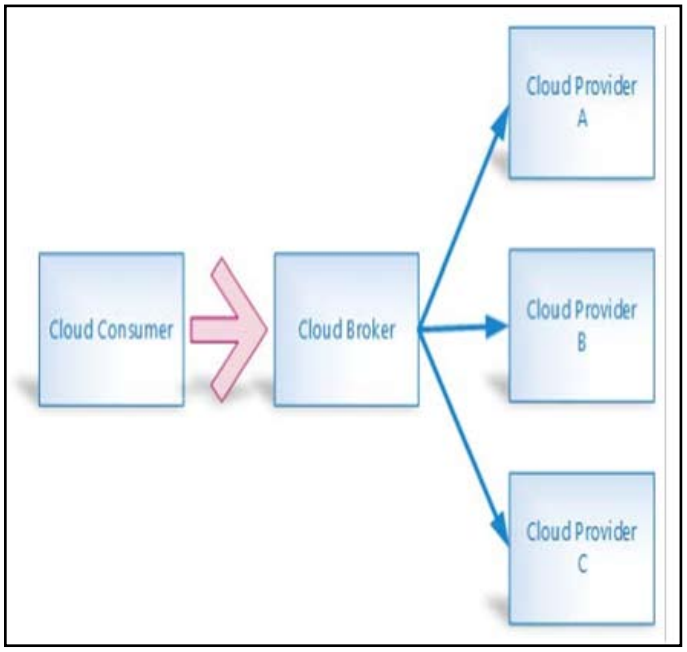

Fig. 4: Cloud Broker

The Approach implementation that secure VMs:

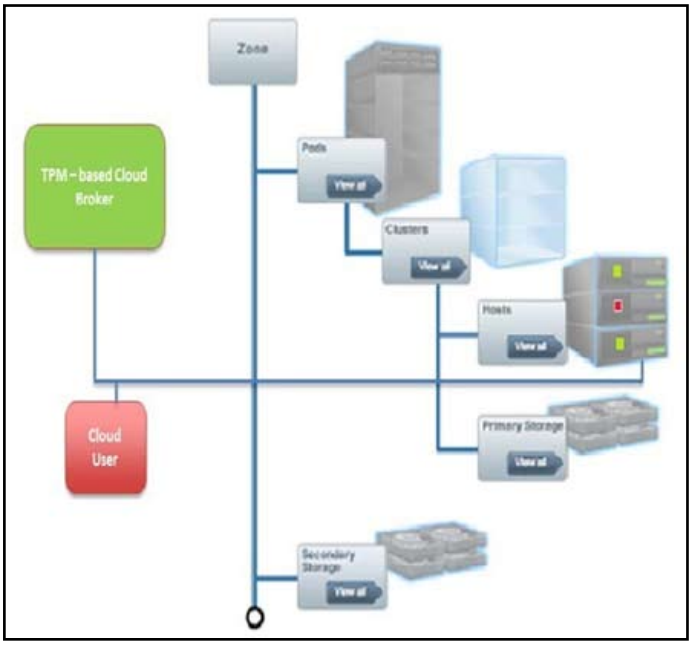

Fig. 5: TPM based solution system

The following figure describe the request and the upload procedure of the client virtual machine image to the CSP

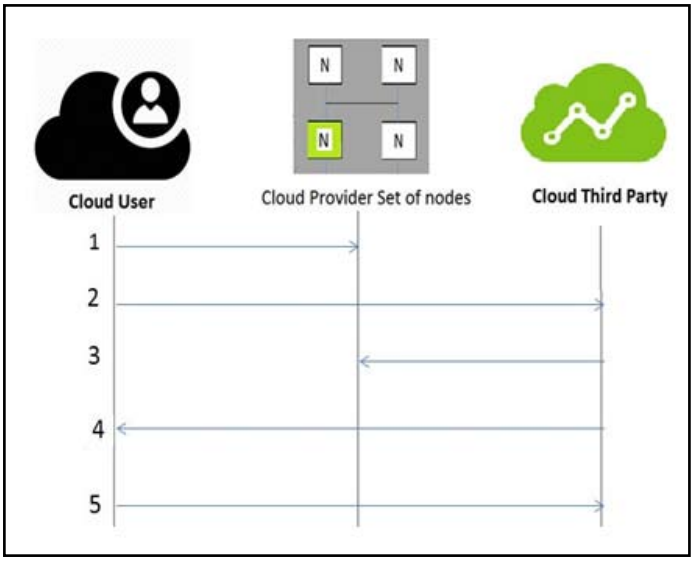

Fig 6: scenario of our approach

Our Approach Scenario:
Before going any further, our approach enforces the virtual machine to be installed in one and only one node, so the insider will have no way to get the customer information. Also, it will be endowed with alert system that will notify the cloud customer in case someone wanted to have access to his data, programs or backup version. If happening, the customer will be recommended to report it immediately to the cloud provider head manager.

Based on The above figure, we will describe the flow of events in our approach scenario:
First, the client requests the IaaS service from the cloud and the cloud broker will analyze the request and then send it to the adequate cloud provider that will later on assign a trusted node to the client.

1. Client ask the cloud provider for the public key of the assigned node's TPM.
2. Matching request of identification keys (AIK) will be sent from client to the Trusted Third Party.
3. Trusted Third Party check if he has this node within his set of trusted nodes using its Pk.
4. Validation of the node as trusted.
5. The client sign it's NAik(VM) and send it to the node

After completing this process, the E ndorsement Key (EK) of the TPM will decrypt the virtual machine endorsement key(NAik(VM)).

Conclusion

In this paper, we proposed a design of trusted deployment of cloud computing that is suitable for companies who are willing to move to Cloud and explore its different services. Our solution secure the client virtual machine image and prevent the insider attacks. It insures a confidential execution of users programs and applications also it allows the users to check how trusted is the IaaS provider before launching and deploying their virtual machines. Our future work ,we are planning to implement a model that uses the trusted platform module widely for the security of cloud/remote storage. We will design a new trust model which uses TPM to store encrypted data to the cloud, in order to make the data safe in the public cloud .

References

[1] *S.Sajithabanu and E.George Prakash Raj, "Data Storage Security in Cloud," InternatIonal Journal of Computer Science and Technology, ISSN: 0976- 8491 (Online)| ISSN: 2229-4333 (Print), IJCST Vol. 2, Issue 4, oct. -Dec. 2011.*

[2] *[10] Hari Baaskar R and Gomathi A, "A Framework for Security Based Cloud by using Trusted Computing," International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277128X, Volume 2, Issue 12, December 2012.*

[3] *[11] Nashaat el-Khameesy and Hossam Abdel Rahman, "A Proposed Model for Enhancing Data Storage Security in Cloud Computing Systems," Journal of Emerging Trends in Computing and Information Sciences, ISSN 2079-8407, Vol. 3, Nn. 6, June 2012.*

[4] *Senk, C.; Dotzler, F., "Biometric authentication as a service for enterprise identity management deployment: a data protection perspective," Availability, Reliability and Security(ARES), 2011 Sixth International Conference on , vol., no., pp.43,50, 22-26Aug. 2011.*

[5] *Shuai Han; Jianchuan Xing, "Ensuring data storage security through a novel third party auditor scheme in cloud computing," Cloud Computing and Intelligence Systems (CCIS), 2011 IEEE International Conference on , vol., no., pp.264,268, 15 -17*

[6] *Bentajer, A. Abouelmehdi, K., Dali, L. (2015). "An Assessing Approach based on FMECA methodology to evaluate security of a third party cloud provider", Journal of Theoretical and Applied Information Technology 30 April 2015 | Vol.74 No.3.*

[7] *Dali, L., El-Sayed, H., Abouelmehdi, K., and Fatiha Eladnani (2015). "The Benefits of The Duo IPv6 and TPM to Enhance the Cloud Security", The 2nd World Symposium on Computer Networks and Information Security 2015, WSCNIS'2015, IEEE Xplore, Tunisia, Sept. 2015.*

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

[8] Boampong, P.A., Wahsheh, L.A. (2012). Different facets of security in the cloud. In: Proceedings of the 15th Communications and Networking Simulation Symposium, pp. 5:1–5:7. Society forComputer Simulation International, San Diego, CA, USA.

[9] TPM Main Specification, Part 1: Design Principles, ver. 1.2, Trusted Computing Group, 2003.

[10] M. Burnside and A.D. Keromytis, "F3ildCrypt: End- to-End Protection of Sensitive Information in Web Services," Proc. 12th Int'l Conf. Information Security (ISC), pp. 491-506, 2009.

[11] [17]. Trusted Computing Group, https://www. trustedcomputing group.org/home, 2013.

[12]. S. Berger et al., "TVDc: Managing Security in the Trusted Virtual Datacenter," ACM SIGOPS perating Systems Rev., vol. 42,no. 1, pp. 40-47, 2008.

[13] J. Garay and L. Huelsbergen, "SoftwareIntegrity Protection Using Timed Executable Agents," Proc. ACM Symp. Information, Computer and Comm. Security (ASIACCS), Mar. 2006.