International Conference on Inter Disciplinary Research in Engineering and Technology [ICIDRET]

ISBN	978-81-929742-5-5
Website	www.icidret.in
Received	14 - February - 2015
Article ID	ICIDRET043

Vol	I
eMail	icidret@asdf.res.in
Accepted	25 - March - 2015
eAID	ICIDRET.2015.043

Dependability Assurance through Trusted Execution of Boot Processing For Infrastructure Security in Cloud Environment

Udayakumar Shanmugam[1], Saranya R[2], Dhinakaran K[3]
[1]Adulhauman University, [2]Saveetha School of Engineering, [3]Saveetha School of Engineering

Abstract - *Cloud delivers on demand services through virtualized infrastructure; however there are variety of security challenges that suppress the growth of it. One of the key security issues are protecting the virtual machine from threats posed by other Vm's so as to ensure a reliable Infrastructure as a service. So we propose a security model for IaaS wherein the VM's dependability is ensured through trusted computing. The hardware root of trust provided as the secure layer beneath the VM ensures cryptographic encryptions, while our layered software process assess through the behavioral pattern of VM. The configuration of the root of trust is extended to the software by having management and monitoring policy. The behavior model checks for any pattern of SLA breaches and checks to verify it authorization. Thus any misbehaved VM will eventually be trapped, and all it services will be put to anti-trust auditing. Thus our trusted execution assures dependability for Infrastructures in cloud environment.*

Keywords: Virtualization, Trusted Platform Module, Homomorphic Encryption.

I. INTRODUCTION

Processing capacity requirements and storage capacity requirement with respect to computing resources are mandatory and changes by the minute in the IT industry. Due to the macro-economic and micro-economic scenario in the current market, the stress on cutting costs and reducing overhead has been the pressure points for market leaders. This pressure point is being handled by a new technology called as CLOUD Computing. The cloud resources are availed by the end user on demand. This provides the organization to move from CAPEX tradition to OPEX tradition (Cloud & shared infrastructure and pay as you go approach).

Cloud computing environment creation is a process of deploying a set of servers and software networks that utilizes a common and central data storage space and also online access to computer resources. Based on user requirements, the providers can be categorized into infrastructure providers (those who manage platform & resources) and service providers (rent resources to users). The cloud can be categorized into (1) public cloud, which has a 'pay as you' subscription model & pay for only consumed resources and (2) private cloud, which are maintained and controlled by a particular enterprise.

Virtualization is a technique, which splits physical resources to create dedicated individual infrastructures. It is the core fundamental technology that is at the heart of cloud computing. "It is possible to run different operating systems and various applications on multiple platforms on the same server at the same time using virtualization technology. It is primarily meant for private cloud, which provides the client with its own virtualized environment having an advantage of more control and flexibility of handling their own operations.

Infrastructure as a Service (IaaS) is a division of Cloud computing, which contains a third party provider hosting virtualized environments and computing resources like physical hardware, server, storage space, network and software's, through the Internet as a service payable on demand. IaaS provides a generic server with common hardware and software for which the end user owns up

Cite this article as: Udayakumar Shanmugam, Saranya R, Dhinakaran K. "Dependability Assurance through Trusted Execution of Boot Processing for Infrastructure Security in Cloud Environment." *International Conference on Inter Disciplinary Research in Engineering and Technology* (2015): 262-268. Print.

responsibility for configuring and installation of another operating system (OS), database and other software's. Computational capacity like performance and storage are also provided on a standard basis. IaaS platform generally provide customizable and highly scalable systems and can be scaled on-demand. IaaS also provides dynamic resource allocation for scaling, desktop virtualization and automation of administrative process.

Leading IaaS providers in the industry comprises of Google Computing Engine, Windows Azure, Amazon Web Services, Rackspace Open Cloud and IBM SmartCloud Enterprise.

II. RELATED WORK

Cloud security means a broad set of technologies, policies and controls implemented to protect data, applications and related resources of cloud computing. The following points show the significance of security and privacy concerns that needs to be addressed:

1. Storing the identity of every enterprise to protect the access restrictions to specified resources and information through their own identity management system.
2. The physical security of data centers is more important for provision of professional data centers in the cloud.
3. Personnel security should be adhered to by other activities like conducting background security checks, training programs, disciplinary procedures and employment contracts.
4. The providers should guarantee the availability of service to users so that they can depend on the applications and resources.
5. The providers should ensure safety of cloud resources by encrypting stored data and running scans at regular time intervals in the production environment.

A. Issues in Cloud security

The security issues in cloud computing can be classified into:

(1) Issues faced by providers of cloud services and (2) Issues faced by the end users. To mitigate these issues, the providers must ensure secure access to the resources of their customers while the customers should also participate by following security good practices. When an enterprise hosts its data in the public cloud, the enterprise is risking its confidential business information. The hosted data centers should be thoroughly for suspicious activities. The providers store multiples customer's data on same server in order to cut cost efficiency and maintain efficiency, which might lead to situations in which one customer might have access to other's private data. These issues should be avoided by following proper logical data storage segregation and isolation techniques.

Virtualization adds a new layer between the Hardware and the Operating System. The new "*virtualization layer*" must be properly setup, configured and managed to avoid security incidents. The issue of compromising the virtualization layer (or) the hypervisor is largely theoretical but certain techniques do exist to exploit such scenarios.

B. Issues for Cloud Computing

Software-as-a-service (SaaS) security issues
SaaS offers services on demand so the customers have little control over security in all the three different models of Cloud computing. The adoption of SaaS applications will have direct impact on security incidents & security audits.

Platform-as-a-service (PaaS) security issues
PaaS offers application services without the underlying cost of buying hardware and software components. PaaS cloud application security comprises of (1) Security of Runtime engine / platform (2) Security of applications installed on the platform.

Infrastructure-as-a-service (IaaS) security issues
IaaS offers a host of resources like servers, networks, and other virtualized systems all accessible over the Internet. The only security concern in IaaS is with the security loophole in the VM (virtual machine) monitor. Since all controls are given over to the user, customer has to spend lot of efforts to maintain the environment without any potential security threats / incidents.

Application and Data security
All the cloud applications are delivered through the web browser. The attacks are also being targeted at the web browsers to steal sensitive business information. The data security of the customer organization is the responsibility of the cloud service provider.

Accessibility
Cloud based application provide universal access to them through web browsers and ease of access and usage. However, the same will also introduce host of security risks such as data theft, insecure marketplaces, proximity hacking and inherent vulnerabilities found in device OS.

Underlying infrastructure security

Underlying infrastructure of PaaS services should be protected by the cloud provider since the developers will not access. Even when they have access, developers cannot ensure the development environment tools offered by PaaS providers are completely safe and secure.

Virtualization

Users can share, copy, migrate and create virtual machines to execute different applications on a cloud resource through virtualization. At the same time, it introduces new venues for security attacks since a flaw in either of the machines (cloud or local) might affect the other as well. Security is a primary challenge in Virtualization because Virtual Machines have physical boundary as well as virtual boundary.

Virtual machine monitor

The hypervisor, also known as Virtual Machine Monitor takes care of the isolation function of virtual machines. In case, of the hypervisor or VMM is compromised, all the VMs are potentially compromised as well.

Shared resource

VMs residing on the same physical server can share resources like processing capacity, storage, input-output modules. Sharing the resources makes each individual VM more vulnerable. For example, a malicious VM can infer some information about other VMs on the same server without the necessity for compromising the VMM or hypervisor. Two VMs can communicate privately bypassing all security rules framed and implemented by VMM.

Public VM image repository

In IaaS environments, a VM image is used to create multiple VMs. These VM images are critical to the overall security of the cloud environment. A user can create their own VM image or use one of these from provider's public repository. In case of an affected VM image having malicious code, malicious users can monitor data flowing through that VM image and record passwords and encrypted data. The IaaS environment is compromised until the infected VM image is cleaned.

Virtual machine rollback

Virtual machines can be reverted back to the last saved restoration point if an error occurs. But the rollback process will restore everything and might expose the VM to already patched security vulnerabilities. For the purpose of rollback, a snapshot ('copy') of the VM needs to be created which will result in the propagation of security vulnerabilities and configuration issues.

Virtual machine life cycle

It is very critical to understand the lifecycle of a VM and its changes while they move through the environment. Virtual machines can be vulnerable even when they are offine.ie. a VM can be instantiated using an image that might have infected code.

Identity and access management guidelines

Cloud Security Alliance (CSA) has issued an Identity and Access Management Guidelines which furnishes a set of recommended best practices to ensure identities and secure access management. This report includes centralized directory maintenance, access level management based on user level roles, role-based access restriction, user access permissions, privileged user and access rights, and access custom reporting.

Fragmentation-redundancy-scattering (FRS) Technique

FRS is a technique used to ensure secure storage of data and also provides tolerance against intrusion attempts. This technique includes splitting the sensitive data into insignificantly small fragments so that a fragment by itself will have no useful information. The fragments are stored in redundant manner across different locations of a distributed system.

Digital signatures

A digital signature is used to sign packets of data to ensure data integrity and security. The RSA algorithm is one of the most popular algorithms used to protect information in cloud based environments.

Homomorphic encryption

The fundamental operations in cloud based processing are (1) Transfer, (2) Store (3) Process. Encryption techniques like hashing, ciphers are employed to secure the data while being transferred or stored in provider's infrastructure. Cloud providers have to de-crypt the encrypted data to enable processing of the same, which heightens security concerns.

Fully homomorphic encryption allows performance of random computation on cipher texts without being decrypted. Current homomorphic encryption techniques support only a limited magnitude of homomorphic operations like addition and multiplication.

Encryption

Encryption techniques have been employed to secure sensitive data in applications. Transmission or storing encrypted information ensures data security. The fundamental assumption about data security is that those algorithms are uncompromisingly strong. Encryption techniques like AES, MD5 hashing, SHA hashing are implemented. Also, Secure Socket Layer (SSL) technology is used to ensure data security during transmission.

Web application scanners

Web applications are an easy target due to its exposure to everyone including potential attackers. Web application scanner is an application program which scans web application through front end to identify security loopholes and vulnerabilities. Web application re-routes all the passing web traffic through the web application firewall which examines the traffic information for specific threats.

HyperSafe

HyperSafe is an approach that gives hypervisor with integrity of control flow. HyperSafe's target is to secure Type-I hypervisors using two methods: (1) non-bypassable memory lockdown (2) Restricted pointed indexing.

Non-bypassable Memory Lockdown secures write-protected memory pages from being changed.

Restricted pointed Indexing secures data by converting control data into pointer indexes.

Trusted cloud computing platform

TCCP is a technology that makes Cloud providers to offer closed-box execution environments and allow users to decide if the Cloud environment is secure before launching their VMs. The TCCP inserts two fundamental elements: (1) Trusted Virtual Machine Monitor (TVMM) and (2) Trusted Co-Coordinator (TC). The TC manages a list of trusted nodes that runs TVMMs and is maintained by a trusted third-party. The TC engages in the process of launching or migrating a Virtual Machine (VM), which will verify that a VM is running on a Trusted Platform.

Trusted virtual datacenter

Trusted Virtual Datacenter (TVDc) ensures logical data isolation and data integrity in Cloud environments. It combines VMs that have common objectives into workloads called as Trusted Virtual Domains (TVDs). TVDc provides isolation between workloads by implementing hypervisor-based isolation, protected communication channels like VLANs. TVDc ensures integrity by implementing load-time attestation mechanism and to verify the integrity of the system.

Protection aegis for live migration of VMs (PALM)

Protection Aegis for Live Migration (PALM) is a secure live migration framework that preserves integrity and privacy protection during and after the migration. The prototype of the system was created based on Xen and GNU Linux. The results of such an evaluation highlighted that such a technique marginally increases the downtime and migration time due to the encryption and decryption.

VNSS

VNSS is a security framework, which customizes security policies for individual virtual machine and it provides continuous real time protection through Virtual Machine Live Migration. They have implemented a system prototype based on Xen hypervisors using state-ful firewall technologies and user space tools like IP Tables, XM commands program and CONN-TRACK tools. The security policies defined are working throughout live migration phase.

Virtual network security

Virtual Network Security (VNS) presents a virtual network framework that ensures secure communication between Virtual Machines. The VNS framework is based on Xen, which offers two configuration modes for virtual networks. (1) "Bridged" and (2) "Routed". The virtual network model comprises three layers: (1) Routing Layers (2) Firewall (3) Shared Networks. All the above 3 layers can prevent sniffing and spoofing from other VMs in the same physical machine.

III. SECURITY CONSIDERATION FOR IaaS CLOUD

Latest survey and poll results clearly highlight that security will remain a major concern for enterprises to move into Cloud infrastructure. Despite the survey, companies are increasingly implementing Infrastructure as a Service (IaaS) without giving much needed attention to the topic of IaaS security,

According to expert analysts at TechNavio, the worldwide market for IaaS is expected to grow at a Compounded Annual Growth Rate (CAGR) of about 45% between 2012 and 2016. There is a recent survey that highlighted many organizations that have not been practicing due diligence when it comes to selecting cloud providers.

1. Considering the data,
   - Classify the data that will be processed in cloud environment
   - Sensitivity of the data
   - Intellectual Property Value of the data

- Transaction processing procedures
- Subject to regulations such as Payment Card Industry's Data Security Standard?
- Application of Privacy Restrictions for the data

2. Define the security procedures that are mandatory to secure the information and ensure that the cloud service provider that they are using have those effective procedures in place. This procedure includes both logical and physical access controls.
3. Organizations must consider their rights under the contract with service provider and their right to audit the security controls with service provider.
4. Organizations must protect themselves from rogue cloud usage (employees abusing their service) and redundant cloud providers.

A. Security in Public IaaS Cloud

1. **Secure all devices connected to Open Internet from unauthorized access**
   - Creation of complex and secure password, changing the password at regular intervals and maintaining different password combinations for different types of devices
   - Since server is not located behind a firewall, it allows the user to set up one's own server and networking to configure it to work without external interference.
   - It is generally advisable to have SSH turned off initially. When users boot up, access via remote sharing tools and reset the default passwords before accessing the machine from external network.
   - For a multi – server setup, addition of servers to a VLAN (Virtual LAN), an additional networking card is added to the server.

2. **Securing the data in transmission across the network**
   - One user will not be able to monitor internet traffic of another
   - The user network traffic is separated at Hypervisor level.
   - The probability of Hypervisor getting compromised is high. So, all private traffic routed over a physical network while all traffic between public IP addresses are routed through another separate physical network.

3. **Ensure high quality reliable networking to the Cloud**
   - The multi-tenant public cloud environment will have unpredictable network traffic that can drastically vary on a hourly basis.
   - The responsibility of IaaS is to ensure best quality cloud service round the clock.
   - Round the clock service availability should be ensured through two measures - (1) Pre-cautionary measures and (2) Reactionary measures.
   - With precautionary measures, the balance should always be maintained between preventing abusive usage of network and interfering with genuine customer traffic.

B. Five Essential Considerations for Securing IaaS Cloud

1. Vendor Selection of IaaS Cloud
2. Frequent Application Integration and Vulnerability Scanning
3. Access and Identity Control Management
4. Log Monitoring and Management
5. Data Encryption

C. Other Attacks in cloud infrastructure

- ***Side channel attack***
  - Infrastructure as a Service (IaaS) model in cloud computing offer infrastructures like a collection of multiple computers, virtual machines (VMs) and other resources to the customers to store their application, file, confidential information, documents…etc.
  - It is probable to map the internal cloud infrastructure and identify the location of a target VM, and then instantiate new VMs until one is located as a co-resident with the target VM.
  - After the successfully placement of new VM with targeted VM, the process of extracting the confidential information from the target VM is called as Side Channel Attack.
  - Side channel attack requires two main steps: Placement and Extraction. *Placement* refers to the attacker working to place their malicious VM on the same physical machine. After successful placement of the malicious VM with the target VM, the process to extract the confidential information, file and documents from the target VM is called as *Extraction*.

- The defense against the vulnerabilities of side channel attack in cloud computing might be mitigated by the combination of firewall and random encryption decryption techniques.

- ***Malware-Injection Attack Solution***

- When a customer opens an account in the cloud, an image of the customer's VM in the image repository system of the cloud is provided by the provider.
- The applications run by the customer are considered with high efficiency and integrity. Consideration of the integrity in the hardware level should be taken into account, because it is very difficult for an attacker to intrude in the IaaS level.
- File Allocation Table (FAT) system architecture is utilized, since its straightforward technique is supported by all existing virtual operating systems. Checking the previous instances that had been already executed from the customer's machine can be put to determine the validity and integrity of the new instance
- Hypervisor must be deployed at cloud service provider's end for the integrity verification purpose. The Hypervisor will be considered the most secured and sophisticated part of the cloud system whose security cannot be breached by any means.
- The Hypervisor is responsible for scheduling all the instance services, but before scheduling any of the services, it will check the integrity of the instance from the FAT table of the customers VM.

D. About TPM chip

Trusted Platform Module (TPM) acts as a technology to answer the security based issues in the form of hardware-based, security-related functions. To achieve the security, TPM chip acts as a crypto processor to perform cryptographic actions. The generation and protection of keys is an important task of TPM for E.g., key or crypto operations such as Unique TPM's RSA key for platform authentication are burned into itself make the denial for malicious software to tamper the security of VM. In a boot processing of a system, the boot code which is loaded and stored in TPM, this could be utilized only if exact software was used to boot. The TPM provides additional functionality to enhance the security such as remote attestation and sealed storage,

IV. PROPOSED SYSTEM

The motivational point for virtual machine begins in the thought for making the single operating system to be a version of multiple operating systems by sharing the same resources with each other to possess the feel about compatible working environment to the user. This phenomena of virtualization provided the top for built the era of cloud computing. Virtualization provided a comfortable platform to the cloud services to improvise the utilization of resources and reduce the cost.

But VM is not a remarkable one in various aspects such as security aspects, less efficient than actual machine, unstable performance during multiple VM execution. The various attacks are:

A *VM escape* is designed to compromise the hypervisor of underlying infrastructure while VM hopping is one VM able to get access to another VM through hypervisor vulnerability.

An attacker with *valid VM account* can create a VM image with malicious code like Trojan Horse and host them in the provider's repository.

A *live VM migration* poses the risk of exposing the entire contents of VM files to everyone on the network. An attacker can illegally access data of VM; transfer VM to untrusted host; creating several VMs causing Denial-of-Service (DoS).

An attacker from an infected VM can *spoof / listen to the virtual network* (or) poison the ARP and spoof packets to other VMs.
To achieve the dependability of VM, software assistance is needed for TPM enabled system for avoiding the Malware protections. The assistance use homomorphic encryptions for creating TPM's cryptographic keys improve the security of VM environment and that encrypted key acts as an additional authentication core during the VM hopping. This software provides the additional layer of security that will avoid malicious users to take the entire control of underlying infrastructure if the hypervisor is convinced. This software may acts as a proxy to avoid the illegal data access during the live migration.

IV EXPERIMENTATION AND RESULTS

The basic implementation starts as creating a virtual environment by three virtual machines in an Intel I7 processor system. Installation of CloudSim Simulator creates netbeans environment in that code should be given to simulate the functionality of TPM as software. The TPM functionality is marked as three modules named as

a. cryptographic processor to create the crypto keys using RSA algorithms, SHA-1 Algorithms along with random number generator and encryption-decryption engine,
b. Persistent memory – acts as a place to store the key generated for ownership along with Endorsement Key to identify the unique platform.

c. Versatile module – consists of registers that store the value needed for integrity, keys generated by RSA for user initialization and attestation environment.

Finally, the functionality of TPM is achieved in a software version of implementation using CloudSim.

V. CONCLUSION

Virtual machine in cloud has greater implications in the success of cloud deployment. Thus our work enables a layered architecture to assure the dependability of cloud's VM. Since VM's are the blackbox of the cloud services, its security should be our highest priority. Hence we presented various security aspects related to VM like Trusted root of execution initiated through hardware boot process using TPM chips and also implementing homomorphic encryptions to safeguard it. Thus our work enhances the security of the IaaS in cloud for a better VM instantiation.

REFERENCES

[1] QianLiu, ChuLiangWeng, MingLuLi, and YuanLuo," An In-VM Measuring Framework for Increasing Virtual Machine Security in Cloud", COPUBLISHED BY THE IEEE COMPUTER AND RELIABILITY SOCIETIES", NOVEMBER/DECEMBER 2010

[2] Rahul Ghosh, Francesco Longo, Flavio Frattini, Stefano Russo, and Kishor S. Trivedi," Scalable Analytics for IaaS Cloud Availability', IEEE TRANSACTIONS ON CLOUD COMPUTING, VOL. 2, NO. 1, JANUARY-MARCH 2014.

[3] Robert Basmadjian, Hermann De Meer, Ricardo Lent and Giovanni Giuliani "Cloud computing and its interest in saving energy: the use case of a private cloud", Journal of Cloud Computing: Advances, Systems and Applications 2012.

[4] Robert Denz and Stephen Taylor," A survey on securing the virtual cloud", Journal of Cloud Computing: Advances, Systems and Applications 2013.

[5] Roland Schwarzkopf, Matthias Schmidt, Christian Strack, Simon Martin and Bernd Freisleben "Increasing virtual machine security in cloud Environments" ", Journal of Cloud Computing: Advances, Systems and Applications 2012.

[6] Russell A. Fink, Alan T. Sherman, and Richard Carback," TPM Meets DRE: Reducing the Trust Base for Electronic Voting Using Trusted Platform Modules", IEEE Transaction on Information Forensics and Security, Vol. 4, No. 4, December 2009.

[7] Sheikh Mahbub Habib, Sascha Hauke, Sebastian Ries and Max Muhlhauser," Trust as a facilitator in cloud computing: Asurvey", Journal of Cloud Computing: Advances, Systems and Applications 2012.

[8] Stumpf, F.; Eckert, C," Enhancing Trusted Platform Modules with Hardware-Based Virtualization Techniques" Emerging Security Information, Systems and Technologies, 2008. SECURWARE '08. Second International Conference on Date 25-31 Aug. 2008.

Cite this article as: Udayakumar Shanmugam, Saranya R, Dhinakaran K. "Dependability Assurance through Trusted Execution of Boot Processing for Infrastructure Security in Cloud Environment." *International Conference on Inter Disciplinary Research in Engineering and Technology* (2015): 262-268. Print.