Towards a Secure Cloud Computing Infrastructure

Sarfraz Brohi, Mervat Bamiah, Suriayati Chuprat
Universiti Teknologi Malaysia, Malaysia
nbsarfraz2@live.utm.my
abmervat3@live.utm.my,suria@ic.utm.my

Jamalul-lail Ab Manan
Mimos Berhad, Malaysia
jamalul.lail@mimos.my

***Abstract*—Cloud computing is considered as a flexible business and technological model for providing an efficient operating environment due to its significant features such as scalability, flexibility, availability disaster recovery, software-on-demand, and accessibility. Since cloud computing is an open access global technology, there are several security threats that might take place from malicious users. Clients are reluctant to trust and adopt this paradigm because of threats that can compromise the security of their confidential data which results into a major barrier for adopting the cloud paradigm. In this research paper, we emphasize the significance of cloud computing and propose a conceptual model for developing a Secure Cloud Computing Infrastructure (SCCI). Our contribution consists of several security tools and techniques such as Trusted Virtual Domains (TVDs), Security as a Service (SECaaS), Intrusion Detection Tools, Trusted Platform Module (TPM), virtual TPM (vTPM).**

***Keywords*- Cloud Computing, Security and Trust Issues, TPM, vTPM, TVD, SECaaS**

I. INTRODUCTION

Cloud computing refers to a business model that has inherited the benefit of other technologies such as distributed, pervasive, ubiquitous, utility computing and virtualization to offer cost effective and scalable IT services to industries, organizations and individuals [1-2]. Cloud computing provides significant cost-effective and attractive services to the organizations that are described in further detail as follows.

A. Scalability and Flexibility

According to the proposed business model for cloud computing, users only pay for the computing resources they use. No need to buy new hardware, software or pay for maintenance and upgrading, only need to pay for the amount of services used. In the past and some existing solution, they need to purchase the infrastructure utilities at a fixed cost that normally became an issue of under or over-utilized infrastructure. Being a client of cloud services, an organization can just acquire the basic resource such as applications, software or data storage size and they can scale up or down whenever is required on-demand. Scalability also allows for rapid escalations in demand at peak times. Therefore, there is no need to plan usage levels in advance [3]. In short, an organization can simply have the flexibility of expanding or shrinking their infrastructure without any loss or management effort.

B. Availability and Disaster Recovery

Cloud Service Providers (CSPs) also provide the required disaster recovery infrastructure and plan [4-5]. They provide recovery system and replication of data at several geographical locations such as cities, countries or states that are permitted by law, and they maintain procedures for the accurate and reliable retrieval of data [6]. Due to disaster recovery plan organizations can safely assume that they are highly saved from facing downtime issues and loss of data because of efficient troubleshooting tools and procedures used by the CSPs.

C. Software on Demand

Organizations can deploy their applications on Cloud Computing Infrastructure (CCI) that can be accessed anytime remotely without installing or configuring them. They don't need to worry about backing up or losing their data as it should be safely stored in the cloud with large storage capacity provided on pay-per-use basis. Client's data and applications can be accessible from any location via range of heterogeneous devices and they never face issues regarding downtime or scheduled maintenance disturbances [1] also they are not required to pay for licensing cost, installation and upgrading of applications.

D. Pervasive and Ubiquitous Accessibility

The systems deployed on a CCI, can be accessible online from any electronic device interface such as smart phones, tablet, notebook, laptops or PCs anytime and from any location. [7]. If organizations are always using the cloud based systems and storing their data on cloud, they are not required to carry backup or storage device, their workload will be saved on the cloud storage and will never get lost due to use of backup and recovery services and it can be accessed within the organization, home or across the border.

II. SECURITY: A BARRIER IN ADOPTING THE CLOUD PARADIGM

Although there are significant flexible and efficient features that cloud computing can provide to organizations. However, security on a CCI is not trustworthy and it is rapidly growing concern that needs to be addressed [8]. When data of a client is at the datacenter of cloud CSP, there are obvious chances of security, hack, theft and various malicious activities that can be performed by illegal users such as hackers. Cloud computing datacenter environment is overloaded with trust issues [9]. Before moving to the cloud, organizations need assurance that their sensitive information is protected from compromised security procedures and their applications are available whenever demanded [10] [11]. Due to security and trust issues in cloud computing, organizations are not yet ready to adopt the paradigm of cloud computing which creates a major obstacle to leverage the significant advantages of cloud services. In order to overcome the security issues. In this paper we have provided a conceptual model to develop an SCCI.

III. Related Work

This section describes some of the valuable contributions by the researchers. [12] designed Trusted Virtual Datacenter (TVDc). The aim of TVDc is to provide a safety net that reduces the risk of security issues that take place by misusing the VMs with the help of malicious software. [13] Proposed a trusted VMM with the use of encryption methods. This technique is referred as CloudVisor. It is implemented as a security monitor that runs in the highest privileged mode even more than the hypervisor. Once the CloudVisor runs then it starts the hypervisor that executes in the least privileges mode. In order to enforce protection and isolation, CloudVisor monitors the use hardware by VMM and VMs. CloudVisor uses security authentication TPM for secure boot-up and encryption of VMs data. [14] Proposed the TVMM by using TPM as root of trust by implementing it on Xen hypervisor. The vTPM provides the isolation security between VMs so no any VMs can access the resources of others. [14] Also proposed a page-based encryption method. This method uses the secret key managed by the hypervisor to encrypt all pages. Encryption uses AES-128 in CBC mode, and hashing uses SHA-256 before the pages are handed over to Dom0. These are few of the valuable contributions however there is tremendous amount of research being carried out by several researchers for securing the VCCI.

IV. Attack Surface of a Cloud Computing Infrastructure

We have identified two major types of attacks on a CCI i.e. un-trusted malicious VM attack by malicious outsider, and insider's attack by a malicious cloud administrator as shown in Fig.1, indicated by red color lines.

A. Malicious VM / Outsider's Attack

Normally malicious VMs may be belonging to the competitor of an organization on cloud, or CSP. The objective of this VM is to infect the services of an organization in order to issue a DoS attack for their systems. This attack may be carried out to threaten the reputation of CSP. A malicious VM can mainly attack in two methods i.e. attack directly on other VMs and affect the client applications with viruses, malwares, Trojan horses or worms, or attacking on the host OS, if host OS is compromised, attacker can exploit the hypervisor and physical layer to misuse the client VMs and data. These kind of attacks can destroy the overall computing infrastructure because host OS is managing the hypervisor that is responsible for providing significant tasks for the VMs such as start, shutdown, pause and restart the VMs, monitor and modify the resources available for the VMs, monitor the applications running inside the VMs, view, copy, and modify the data stored in the virtual disks assigned to the VMs. This enables the host to monitor all the network traffic for all its VMs [15]. In-case if a host is compromised then the security of the VMs is under question. On the other hand, malicious VM can also change the configuration of underlying hardware and may try to steal the confidential data of an organization. Hence measurement should be taken when configuring the VM environment so that enough security standards should be implemented which avoids the host being a gateway for attacking the VM [15], and physical layer must be protect by illegal access as it should be resistant to any malicious software activity.

B. Malicious Administrator / Insider's Attack

One of the primary security concerns in cloud computing is that the customer loses direct control over potentially business sensitive and confidential data. This needs more attention because the CSP is outside the trusted domain of customer [16]. The risk of a malicious insider is one of the most dangerous security threats. The cloud security alliance report lists malicious insiders as the number three top threat in cloud computing [6]. Clients are not aware and fully trusting the security technique used by the CSP when their data is on open access cloud computing platform. They believe even if their data is protected from outsider's attack but how about insider's attack. It is possible that malicious cloud administrator may, retrieve, view and misuse the confidential data of an organization. In order to gain the trust of an organization, CSP must provide them trustable security standards that ensure the protection of their data-at-rest.

V. Secure Cloud Computing Infrastructure (SCCI)

To address the issues on CCI, we have designed a conceptual model of SCCI on the public CCI that is shared by multiple tenants including trusted and un-trusted user. Trusted user is the organization who has signed a well-defined SLA with the CSP to use the cloud service delivery models such as SaaS, PaaS, and IaaS (Storage-as-a-Service) on pay-per-use billing pattern accessing via smart devices such as Notebooks, Smart phones, Tablets etc. Un-trusted users refer to general public who are registered online with the CSP for using some shared service such as web-mail, media players, games etc as shown in Fig.1 the services of a an organization are running on VMs, we have illustrated the use of two VMs for the organization, both VMs consists on guest OSs and applications that are configured on Apache Tomcat server along with a DBMS such as MySQL. The un-trusted users are also assigned with VMs to access some free services provided by CSP. The client VMs are managed by VMM in our case, we have proposed the use of KVM hypervisor running on a Linux Host OS. Since these VMs of un-trusted users are not trusted, they might be malicious and their target might be to threat the organization or the CSP. The proposed model is divided into two major parts for managing the security i.e. Management of security by CSP and client. CSP is responsible to secure all layers of computing infrastructure against outsider's attacks. Clients are responsible to secure and control their personal data against insider's attacks by acquiring a remote cryptography software using Security as a Service (SECaaS). The proposed model is developed by using several security tools as well as techniques such as SECaaS, TPM, vTPM, Virtual Firewall (VFs), Intrusion Detection Systems (IDS) and TVD to eliminate the threats of malicious VMs on the VMs of organization and to block the insider to view or misuse the data of organization as shown in Fig.1. The detailed mechanism of our security model is further described.

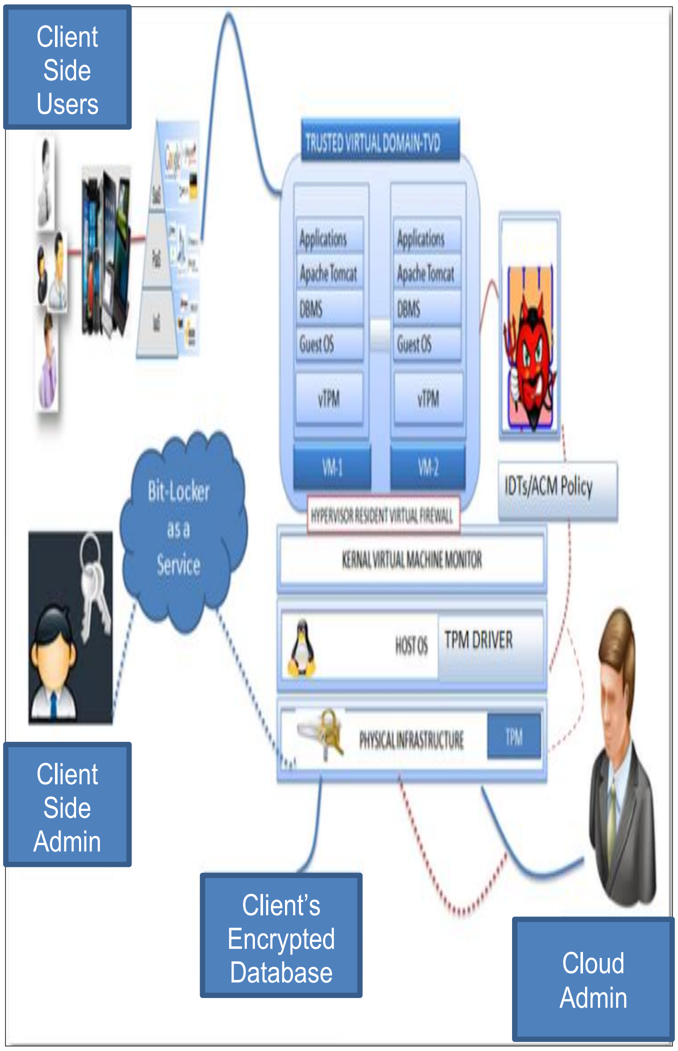

Figure 1. Secure Cloud Computing Infrastructure SCCI

A. *Securing the Virtualization Layer*

We have proposed the use of IDTs, TVD, TPM driver, vTPM and hypervisors-resident VF to secure the virtualization layer that includes VMs and VMM. These tools will be illustrated as follows:

1) *Intrusion Detections Tools (IDTs)*

IDTs will collect and analyze data from a computing system, aiming to detect intrusive actions. We propose the use of two main approaches for IDTs i.e. Network-based IDTs (NIDTs) and Host-based IDTs (HIDTs), NIDTs will monitor the network traffic flowing through the systems whereas HIDTs will monitor the local activities on a host like processes, network connections, system calls, logs, etc and examining events like which files have been accessed and what applications have been executed [17].

2) *Trusted Virtual Domains (TVDs)*

Since isolation is one of the main solutions to eliminate the threat of malicious VMs attacking on VMs of trusted users. In our model, isolation is achieved by using the technique of TVD, which is formed at CCI by grouping the related VMs running on separate physical machine into a single network domain with a unified security policy. The multiple instances of TVDs co-exist on a single platform under a shared resource policy. The use of TVD provides strong isolation among un-related VMs as the communication among VMs will take places only according to the security policies configured by administrator in the VMM. A malicious VM cannot join any TVD because it should fulfil the access policy requirements so no any malicious VM will affect the VMs of trusted users on cloud [18]. Normally the VMs residing in a TVD are labeled with a unique identifier. The labeling is used to identify the assigned VMs to a particular customer and to allow the same labeled VMs to run inside the same TVD.

3) *TPM Driver and vTPM*

In order to protect the KVM hypervisor from attacks of malicious VM, we need to secure the OS kernel. To achieve this, we have proposed the use of TPM driver at this layer. It is a kernel-mode device driver designed for TPM, it will allow the host OS to communicate with hardware TPM that will provide more platform stability and eliminates the need for vendor-specific device drivers. TPM driver can be used in various OSs such as Windows and Linux to protect the OS from attacks **[**19]. If OS is free from attacks the security of hypervisor will remain alive. Since the physical TPM is used to protect the host OS and underlying physical platform and the use of vTPM, it provides same TPM like functionality for VMs, each VM will have its own vTPM instance that will be created by vTPM manager and will keep running throughout the lifetime of the VM which will communicate with underlying TPM through drivers. The use of vTPM will ensure the integrity and consistency of VMs'.

4) *Hypervisor-Resident Virtual Firewall*

Hypervisor-resident VF that is implemented on the VMM and it is responsible to capture malicious VM activities including packet injections. The VF requires a modification to the physical host hypervisor kernel to install process hooks or modules allowing the VF system access to VM information and direct access to the virtual network switches as well as virtualized network interfaces moving packet traffic between VMs. The hypervisor-resident VF can use the same hooks to then perform all firewall functions like packet inspection, dropping, and forwarding but without actually touching the virtual network at any point [20].

B. Securing the Physical Layer

Physical layer is secured by a TPM. Its implementation is available as a chip that is physically attached to a platform's motherboard and controlled by software running on the system using well-defined commands. It provides cryptographic operations such as asymmetric key generation, decryption, encryption, signing and migration of keys between TPMs, as well as random number generation and hashing [21]. TPM also provides secure storage for small amounts of information such as cryptographic keys. Because it is implemented in hardware and presents a carefully designed interface, TPM is resistant to software attacks. Physical layer is secure proof mainly by TPM’s Trusted Execution Technology (TXT), it is a feature of Intel’s microprocessors and chipsets commonly referred to as Intel vPro. It provides a late launch capability for the secure creation and launch of virtual execution environments called Measured Launch Environments (MLEs) that can be launched anytime after a platform is booted. Hardware protections are provided by TXT against software based attacks on MLEs during launch and while the MLE is executing [11]. The use of MLEs will monitor the performance of computing infrastructure and block any possible threats by outsider attackers to underlying hardware.

C. Security as a Service / (Bit-Locker as a service)

By acquiring SECaaS, the administrator from an organization will be able to protect their particular data storage disks by performing cryptographic encryption and decryption operations. This target will be achieved by providing remote access of TPM enabled software i.e. Bit-Locker Drive Encryption as a service to the client. It is a new security feature that provides better data protection by encrypting all data stored on the OS volume. For-example if client’s data is stored on drive “C”, the CSP must enable the client to encrypt that particular drive via Bit-Locker as a Service. Once the client’s admin activates Bit-Locker on their volume, a password will be required that will use a master or private key for the client and upon successful activation, a recovery file will be generated by the software, this file can be used in case of forgetting or losing the master key, the master key and recovery file must be only known to a highly privileged person from the organization such as administrator and should be stored on an isolated device not on the machine at which encryption has taken place. Once the data is sealed by the client the volume will be displayed with golden lock [21] as shown in Fig.1. However, Bit-Locker can only be used with TPM to perform the required tasks such as sealing and unsealing to protect the user’s data. Under this mechanism of SECaaS, the clients will be confident that their data are protected from any insider threat at CSP side.

VI. Conclusion and Future Work

Cloud based solutions are cost-effective in-terms of scalability, availability, on-demand self service, recovery and flexibility. However, there are certain barriers of security that are blocking the organizations from adopting cloud computing. In order to contribute in the field of cloud computing security, we have designed a conceptual security model i.e. SCCI. This model is based on analysis, concepts and theories. However we will focus on providing a practical prototype by implementing the proposed model and evaluation results in our upcoming research publication.

Acknowledgment

We are thankful to God Almighty for giving us the knowledge and wisdom to complete this work. We are also thankful to our parents for their encouraging support.

References

[1] IBM, “IBM Data Center Networking: Planning for virtualization and cloud computing,” International Technical Support Organization, 2011.

[2] Appistry, “Unlocking the Promise of Cloud Computing for the Enterprise Achieving scalability, agility and reliability with cloud application platforms,” [Online] Available from http://charltonb.typepad.com/papers/Unlocking_the_Promise_of_Cloud_Computing_for_the_Enterprise.pdf .

[3] UNESCO, 2010. Cloud Computing in Education, Available from http://iite.unesco.org/pics/publications/en/files/3214674.pdf.

[4] Jadeja, Y.; Modi, K.; , "Cloud computing - concepts, architecture and challenges," *International Conference on Computing, Electronics and Electrical Technologies (ICCEET), 2012*, vol., no., pp.877-880.

[5] iyi Wu; Lingdi Ping; Xiaoping Ge; Ya Wang; Jianqing Fu; , "Cloud Storage as the Infrastructure of Cloud Computing," *International Conference on Intelligent Computing and Cognitive Informatics (ICICCI), 2010*, vol., no., pp.380-383.

[6] CSA, 2009. Security guidance for critical areas of focus in cloud computing V3.0, Available from https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf.

[7] Yau, S.S.; An, H.G.; , "Software Engineering Meets Services and Cloud Computing," *Computer* , vol.44, no.10, pp.47-53, Oct. 2011.

[8] Sultan Nabi, 2010. Cloud Computing for Education: A new dawn? In International Journal of Information Management: Elsevier, pp. 109-119.

[9] Filip A., Rolul, 2011. Stakeholderilor in teoria de marketing relational (The role of stakeholders in relationship marketing theory in Romanian), Calitatea – access la success Journal (Quality1access to success), no. 3, 2011, pp. 27130.

[10] S. Pearson and A. Benameur, 2010. Privacy, Security and Trust Issues Arising from Cloud Computing, in Cloud Computing Technology and Science (CloudCom), 2010 IEEE Second International Conference, pp. 693-702.

[11] F. John Krautheim, 2009. T Private virtual infrastructure for cloud computing, in TRUST'10 Proceedings of the 3rd international conference on Trust and trustworthy computing.

[12] Berger, S., R. Caceres, et al. 2009. Security for the cloud infrastructure: Trusted virtual data center implementation. IBM Journal of Research and Development 53(4): 6:1-6:12.

[13] Zhang, F., et al. 2011. CloudVisor: retrofitting protection of virtual machines in multi-tenant cloud with nested virtualization. Proceedings of the Twenty-Third ACM Symposium on Operating Systems Principles. Cascais, Portugal, ACM: 203-216.

[14] Jinzhu Kong, 2010. Protecting the Confidentiality of Virtual Machines Against Untrusted Host. In Intelligence Information Processing and Trusted Computing (IPTC), 2010 International Symposium on. Intelligence Information Processing and Trusted Computing (IPTC), 2010 International Symposium on. pp. 364–368.

[15] Sengmei Luo, et al., 2011. Virtualization security for cloud computing service, In International Conference on Cloud and Service Computing (CSC), vol., no., pp.174-179, 12-14.

[16] Srinivasan, et al., 2012. State-of-the-art Cloud Computing Security Taxonomies A classification of security challenges in the present cloud computing environment, In: International Conference on Advances in Computing, Communications and Informatics (ICACCI-2012), ICACCI '12, ACM, 2012, Chennai, India.

[17] Harley Kozushko, 2003. Intrusion Detection: Host-Based and Network-Based Intrusion Detection Systems, Available from http://infohost.nmt.edu/~sfs/Students/HarleyKozushko/Papers/IntrusionDetectionPaper.pdf.

[18] Luigi, C., et al. Trusted Virtual Domains – Design, Implementation and Lessons Learned, Available from http://infohost.nmt.edu/~sfs/Students/HarleyKozushko/Papers/IntrusionDetectionPaper.pdf.

[19] Microsoft, 2007. TPM Driver, Available from http://technet.microsoft.com/en-us/library/cc734122(v=ws.10).aspx.

[20] Clement Berthelot, 2011. Evaluation of a Virtual Firewall in a Cloud Environment, Available from http://buchananweb.co.uk/09014406_MSc_VirtualFirewall.pdf.

[21] Microsoft, 2012. Trusted Platform Module Administration Technical Overview, Available from http://technet.microsoft.com/enus/library/cc766159(v=ws.10).aspx