A virtual TPM architecture for providing Infrastructure a service in cloud computing

Tarashankar Rudra
RTC institute of Technology
Ranchi, India

Abstract – A trust platform module has become a standard chip in all high performance computers. In this paper, we present the architecture to implement a system that provides trusted computing by hosting a number of operating systems as virtual machines. Our proposed architecture is implemented on a hypervisor running multiple operating systems.

Keywords IaaS, hypervisor, TPM, NIC, NAT

I INTRODUCTION

In modern cloud computing environment, providing infrastructure as a service is a huge challenge, particularly when it comes to trusting a client who wants access to host resources. Cloud computing has become the fastest growing computing paradigm today. Many companies are providing a large number of services related to storage and application as a service. Adobe and Microsoft have made their premium applications available in the cloud and many government agencies are outsourcing their IT infrastructure to the cloud as a cost cutting measure to provide high quality and reliable services to their clients. One of the disadvantages of cloud services is that it requires a reasonably fast Internet connection and an annual subscription.

In this paper, we propose an architecture for infrastructure as a service for a host installed with a hypervisor, and virtual TPM and virtual network interface cards on virtual machines running different operating systems. The paper is organised as follows, the second section is an introduction to cloud computing, the third section introduces the readers to the three services provided by cloud computing, the fourth section describes our proposed architecture for infrastructure as a services and finally we have the conclusion.

II CLOUD COMPUTING

Cloud Computing frequently is taken to be a term that simply renames common technologies and techniques that we have come to know in IT [1]. It is believed that August 24, 2006 is the birthday of Cloud Computing, as it was on this day that Amazon made the test version of its Elastic Computing Cloud (EC2) public [2]. This offer, providing flexible IT resources (computing capacity), marks a definitive milestone in dynamic business relations between IT users and providers. Amazon targeted developers, who had no wish to hold their own IT infrastructure, and instead, hired the existing infrastructure from Amazon via Internet [3].

Today, much of Cloud Computing is still a vision. This becomes especially evident when questions are raised about security and quality of service, consequently, the providers have to weigh whether the services can also effectively meet the company demands of supporting the business processes.

Professional providers of Cloud Computing for enterprise customers not only face legal challenges in storing customer data without their consent, but also endeavour to develop concepts in order to do so in a transparent, cost-effective manner.

III SERVICES PROVIDED BY CLOUD

Cloud computing involves deploying groups of remote servers or a powerful hypervisor running multiple operating systems and software networks which allows centralized data storage and online access to computer services or resources. Cloud services are divided into three main categories, infrastructure as a service (IaaS), platform as a service (PaaS) and software as a service (SaaS). The services can be classified as public, private or hybrid.
The three services provided by Cloud providers are as shown in figure 1. They are briefly described below [4]:

IaaS: In IaaS, providers offer computers in the form of hypervisor, such as Xen, Oracle VirtualBox, etc that runs on virtual machines as guest users. A large number of hypervisors within the cloud operational support-system that support large numbers of virtual machines are scalable according to requirements of the client. The applications offered to the clients are installed along with the images of the operating-system on the cloud infrastructure. In this IaaS model, the client uses the infrastructure of the provider along with the operating systems and the application software whereas the Cloud providers bill for IaaS services on the basis of the amount of resources allocated and consumed by the client.

PaaS: In the PaaS models, cloud providers offer a computing platform, that includes the operating system, programming language execution environment, database, and web server. Application developers can develop and run their software solutions on a cloud platform without the cost and complexity of buying and managing the underlying hardware and software layers.

SaaS: In this model, users are provided access to application software and databases. SaaS is often referred to as "on-demand software" and is usually priced on a pay-per-use basis or using a subscription fee. In the SaaS model, cloud providers offer their application software through the cloud and cloud users download and access the software from the cloud. Cloud users install the program in their computers and do not have to worry about upgrading to a newer version of the software, neither they have to manage the cloud infrastructure and platform where the application resides. Licensing of the application software are done based on the number of systems the software will be installed. It is extremely beneficial for any business, small to large as they are always up to date with modern technology and do not have to worry about installing the old applications using CDs after a hardware upgrade.

IV ARCHITECTURE FOR IaaS

The architecture for our implementation of IaaS is given in figure 2. In our system, the domains (DOM0, DOM1) run different operating systems with compatible application softwares. It is these domains that are leased to consumers seeking infrastructure as a service.

Implementation

1. DOM TPM is a VM that is started first on the system and is associated with the system’s physical TPM. It makes available the TPM instances to all others VMs running on the system (DOM0 .. DOMn).
2. vTPMs [5] are full software implementations of a TPM for individual VMs.
3. vNICs [6] are full software implementations of a network interface card for individual VMs.
4. NAT stores the virtual address of every VM running in the system.
5. The virtual switch helps in making a connection between the domains and the client.

A virtual switch was introduced by Microsoft to manage the traffic between the VM and the server’s shared resources [7].
Conclusion

We have proposed a robust architecture for implementing IaaS. This architecture is more secure and scalable as modern systems already have core networking infrastructure implemented based on our proposed model on a single operating system. The existing concepts of vTPM and vNIC will implement the functionalities provided by TPM and NIC in a hypervisor providing IaaS.

Bibliography


