Security Techniques for Multi Tenancy Applications in Cloud

Nagarjuna
Department of computer science in KMMIT and member of CSI

C.C kalyan srinivas
Department of computer science and engineering, KMMITS,Tirupathi

S.Sajida
department of Master of computer application, KMMIPS,Tirupathi

Abstract
In cloud-based architectures, multi-tenancy means that customers, organizations, and consumers are sharing infrastructure and databases in order to gain price and performance advantages. At its simplest, the "cloud" is an Internet-based environment of computing resources comprised of servers, software, and applications that can be accessed by any individual or business with Internet connectivity. In the case of these "service" offerings, customers (or "tenants") get a piece of the cloud that contains the resources they need to run their business. Cloud computing is the basis for infrastructure as a service (IaaS) and software as a service (SaaS). These services offer a pay-as-you-go lease style investment with little or no upfront costs versus buying all of the hardware and software outright. Other benefits include the ability to scale easily and tier more services and functionality on an "as needed" basis. The benefits, in fact, are so compelling that cloud computing is predicted by some to be the replacement for traditional means of obtaining these services and business capabilities by 2014. The big concern is how to ensure that proper security and isolation protects consumers or tenants of these services from the risks they pose to one another. Hence to provide security for various applications being run in multi tenancy, we are proposing a model based on segmentation on Hyper-visor, Database in the cloud.

Keyword
Cloud, security, multi tenancy

1. Introduction

Cloud computing changes the way we think about technology. Cloud is a computing model providing web-based software, middleware and computing resources on demand. By deploying technology as a service, you give users access only to the resources they need for a particular task. This prevents you from paying for idle computing resources. Cloud computing can also go beyond cost savings by allowing your users to access the latest software and infrastructure offerings to foster business innovation. In the business model using software as a service, users are provided access to application software and databases. The cloud providers manage the infrastructure and platforms on which the applications run. SaaS is sometimes referred to as "on-demand software" and is usually priced on a pay- per-use basis. SaaS providers generally price applications using a subscription fee. Proponents claim that the SaaS allows a business the potential to reduce IT operational costs by outsourcing hardware and software maintenance and support to the cloud provider. This enables the business to reallocate IT operations costs away from hardware/software spending and personnel expenses, towards meeting other IT goals. In addition, with applications hosted centrally, updates can be released without the need for users to install new software. One drawback of SaaS is that the users' data are stored on the cloud provider's server. As a result, there could be unauthorized access to the data. End users access cloud-based applications through a web browser or a light-weight desktop or mobile app while the business software and user's data are stored on servers at a remote location. Proponents claim that cloud computing allows enterprises to get their applications up and running faster, with improved manageability and less maintenance, and enables IT to more rapidly adjust resources to meet fluctuating and unpredictable business demand. Cloud computing relies on sharing of resources to achieve coherence and economies of scale similar to a utility (like the electricity grid) over a network. At the foundation of cloud computing is the broader concept of converged infrastructure and shared services. The notion of a tenant in the context of cloud computing is not as simple as it might first appear. Take Amazon Web Services (AWS), for example. AWS is a cloud service provider with offerings that span application hosting, backup and storage, e-commerce, and media hosting, to name just a few. Companies like Autodesk, Urban Spoon, and Second Life are tenants of AWS, in that they use AWS storage and compute resources to power their customer offerings. Each firm also has customers who store data like personal preferences, credit cards, and information as tenant users of these businesses. In the case of Second Life, for example, if the tenants set up online businesses and services of their own, they, too, will have tenants and so on. In the final analysis, a cloud service tenant is sharing a resource with a community. And similar to a building tenant, the tenant's space must be separated and isolated from other occupants to achieve a certain degree of security and privacy.

The idea of multi-tenancy, or many tenants sharing resources, is fundamental to cloud computing. Service providers are able to build network infrastructures and data architectures that are computationally very efficient,

Manuscript received August 5, 2015
Manuscript revised August 20, 2015

highly scalable, and easily incremented to serve the many customers that share them. Multi-tenancy spans the layers at which services are provided. In IaaS, tenants share infrastructure resources like hardware, computation servers, and data storage devices. With SaaS, tenants are sourcing the same application (e.g., Salesforce.com), which means that data of multiple tenants is likely stored in the same database and may share the same tables. When it comes to security, the risks with multi-tenancy must be addressed at all layers. The next few sections examine how this can be accomplished for shared hardware and application infrastructure.

2. Multi-tenancy Security Threats

According to Armbrust and Fox (2010) and Feng et al (2011), the fundamental security issue with multitenancy is clients using Cloud Computing by employing single and the same computer hardware to share and process information. This presents a number of challenges in terms of compliance, security, and privacy (Bernardo and Hoang, 2010). The lack of user network isolation, moreover, makes Cloud Computing vulnerable to threats, as does the lack of efficient bandwidth and traffic isolation, since malicious tenants may launch attacks to other tenants in the same cloud data centre. Existing approaches to access control on the clouds do not scale well to multi-tenancy requirements because they are based merely on individual user IDs.

Sharing software and data by multiple clients poses risks, such as Intellectual Property infringement, data infringement, and technical and industrial business sabotage (Bernardo, 2012). Cloud Computing providers therefore are responsible in ensuring that tenants cannot cross and access each other's hosted infrastructures. Another common threat within a Cloud environment is "shrew" attack (Feng, et al, 2011), whereby the extremely low number of packets constituting the attack payload and the extremely short duration of the attack make the attack on fingerprint hard to detect. Additionally, the countermeasures rely on very knowledgeable network administrators for implementation at the core switching and routing points of the CSP's network.

In multi-tenanted environment, the network access required by administrators and users of Cloud-based applications originates from outside of the CSP's network address space. Typically, each tenant requires a discreet set of IP addresses, routable and accessible from the public Internet, in order to access their applications and administration consoles.

The CSP is responsible for managing a limited pool of IPv4 addresses and subnets, and must ensure that each tenant has their own dedicated address.

3. Securing the Multi-Tenant Environment

3.1 Hypervisor-Based Segmentation:

Virtualization is quite often the platform that underpins IaaS offerings. Software, such as VMware vSphere, Citrix XenServer, and Microsoft Hyper-V, provides the means of turning a single piece of hardware into a physical host for many VMs. These virtual machines are the databases, file servers, application servers, and Web servers that comprise the typical physical network, and enable the traffic that makes commerce and communication over the Internet possible. They are also the servers offered to customers of IaaS for storing their data or running their web-based businesses. At its core, the virtualization platform includes a very specialized and optimized OS called the hypervisor, which in part serves to map traffic from VMs to the underlying VM host hardware so that it can make its way through the data center and out to the Internet and vice versa. The majority of security concerns in the virtualized infrastructure relate to the co-residency of machines owned by different customers. This places machines in a privileged position relative to one another. And this can elevate the risk for many types of breaches such as unauthorized connection monitoring, unmonitored application login attempts, malware propagation, and various "man in the middle" attacks.

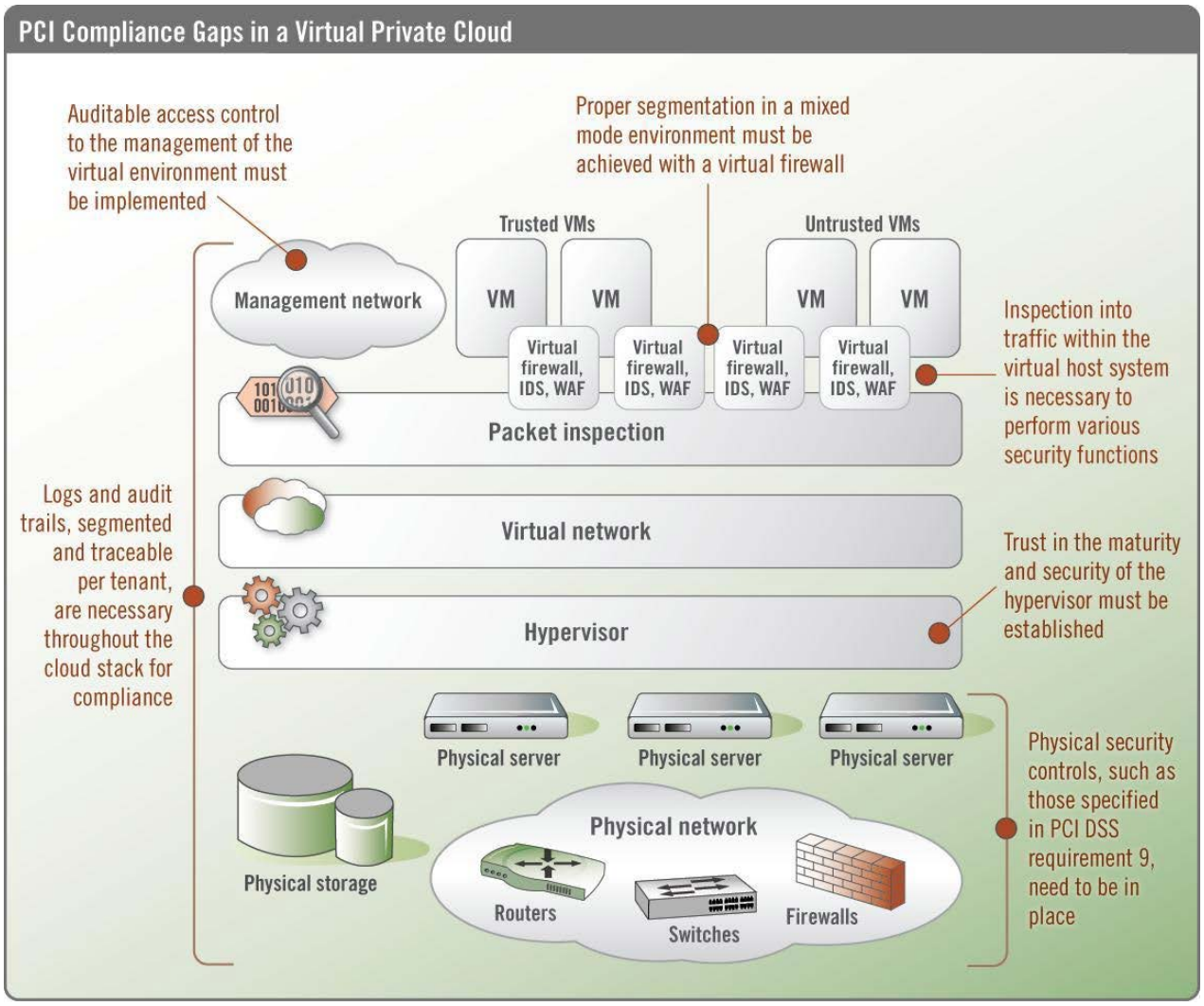
VM segmentation and isolation is also an absolute requirement for VMs containing regulation and compliance intense data like employee details, customer information, etc. Most regulatory mandates such as Payment Card Industry Data Security Standard (PCI DSS), Health Insurance Portability and Accountability Act (HIPAA), Sarbanes-Oxley Act (SOX), and Gramm Leach Bliley Act (GLBA) require that access be limited to a business' need to know, and that control policies be set in place to enforce blocking of unwarranted access. Since the hypervisor intercepts all traffic between VMs and VM hosts, it is the natural place to introduce segmentation for the resources of IaaS tenants where VMs might be housed within the same VM host or VM host cluster.

APIs like VMware VMsafe have enabled an ecosystem of security solutions that embed inside the hypervisor for the purpose of introducing proper segregation, isolation, and protection of tenant resources—thereby enabling secure multi-tenancy. The security solution runs as a service

inside the hypervisor and intercepts traffic or packets. In fact, those products supporting VM Introspection, a concept discussed later in this paper, will also have a great deal of information about the VM's state, including installed applications and services. Depending on the vendor of the security software, the solution may provide virtual network visibility to traffic, VM inventories, and VM compliance assessment, as well as application-based access control and malware suppression.

3.2 Database-Based Segmentation:

Unlike IaaS where multiple tenants share resources, SaaS tenants share a database. Users of Salesforce.com or SmugMug, for instance, pay to use an application that manages their customers and photos respectively. While the value is in the application interfaces that make it easy to manage complex tasks and large data sets, the data itself is stored in a database as rows in tables that the tenants of Salesforce.com and SmugMug databases share. The customer ID is what distinguishes one row from the next. In this area, security concerns run high that misconfigured application code or an error in an access control list may put tenant information at risk of theft and misuse. For controlling access to database data, there are quite a few tools and technologies available. What is usually implemented is a system for authentication and authorization of the access request so that only certain rows or fields are modifiable based on security policies that ensure that access is warranted. Encryption of data in the database is also common to protect it at rest, so that if it is ever compromised or stolen it would be difficult to decipher the underlying data.swq



3.3 The Role of VM Introspection:

Relative to the Internet and network security technologies, virtualization platforms and cloud computing architectures are very new and still evolving. It is important to be aware of innovations that may augment security for multi-tenant environments but may not be broadly known or understood. It is often the case that the standards and reference architectures we rely on for proper implementation lag technological advancement. VM Introspection is a concept that has existed for some time in academic circles and is explained largely as a hypervisor-based service that examines the internal state of a running VM. Technologies have recently been commercialized that leverage VM Introspection in order to provide high levels of segmentation and isolation for guest VMs or cloud service tenants. VM Introspection provides rich detail about the applications and services that are installed on the VM, as well as its configuration. It is possible then to construct security policies on the basis of VM Introspection parameters.

An example of such a policy might be:

Do not allow a new virtual machine to join a VM group or cluster unless it has a specific OS configuration and hot fix installed. VM Introspection takes security for multi-tenancy to a new level where configuration errors are automatically prevented. This becomes especially important in environments where the onus for configuring security and VM isolation falls on tenants, who may or may not have experience in this area.

3.4 Automation as an Enabler:

While security for multi-tenant environments might be the overarching concern for adoption, security automation will be the real catalyst for broad use of cloud-based services. Most will agree that the technologies to secure IaaS and SaaS architectures are broadly available and proven. The real challenge is that the tenants aren't always clear on which type of architecture they are using and what, if any, is their role and responsibility for protecting their information.

Cloud service providers may implement the technologies, but may not fully control how they are managed and configured, as in the case where tenants themselves have sub-tenants. The key to securing multi-tenancy is for anyone who is a tenant (e.g., a business or consumer of IaaS and SaaS on some level) to ask the cloud provider about existing protections and responsibilities for defining and maintaining policies that ensure isolation from other cloud tenants. Also key is to ask how much of the process is automated. Cloud computing environments, especially those based on virtualization, are extremely dynamic. Change is constant, and this makes the likelihood of resource and security misconfiguration high. With available technologies that automate VM protection (at least for IaaS), there is no reason to incur the higher risk, especially given the breadth of current and projected cloud service and provider options.

4. Conclusion

Tenants may share hardware on which their virtual machines or servers run, or they may share database tables. In either case, security measures are "a must" to ensure that tenants do not pose a risk to one another in terms of data loss, misuse, or privacy violation. Multi-tenancy protections must be offered by cloud service providers for all layers of their offerings (i.e., IaaS and SaaS). Cloud service providers owe it to their customers to have the latest and best approaches as available options such as Hypervisor, Database segmentations etc. to enhance cloud security when multiple tenants are sharing the resources.

References:

[1] http://www.juniper.net.
[2] http://en.wikipedia.org/wiki/Cloud_computing
[3] http://en.wikipedia.org/wiki/Managing_Risks_in_Cloud_Computing#Multi-tenancy_Security_Threats