Promises and Challenges of Cloud Computing

Edward S David
Vice President
Applications Development
Citigroup

ABSTRACT

Cloud computing has hit the information technology landscape like a tsunami. But, is it a right strategy? Is it feasible to integrate with enterprise infrastructure? Is it safe and secure? We will examine these questions from various points of views. All of best practices and process for securing and stabilizing the enterprise IT infrastructure still apply with cloud computing. Every multi-national organization has adopted this technology and started thinking of moving more and more IT assets to the clouds. We will explore 3 benefits and 3 challenges of implementing cloud computing from enterprise perspectives. Benefits: 1) Operational efficiency 2) Financial gain 3) Process automation. Challenges: 1) Security Management 2) Vendor Risks 3) Layered cloud architecture

General Terms

Promise and Challenge, Cloud Computing Defined, Layered cloud architecture, Securing VM boundaries

Keywords

IaaS issues, PaaS issues and SaaS issues. .

1. INTRODUCTION

Cloud computing has been top of every technology trend list for quite some time now. As organizations continue to look for more avenues to cut cost and reduce the capital expenditures on IT assets, the focus invariably turned to on-demand/metered computing through shared resources. They are increasingly transitioning from company-owned IT hardware, software and services to cost-effective, agile and flexible IT service model using the latest developments in cloud computing technology. Companies need on-demand computing resources to help them with aggressive business development campaigns; enable multisite collaboration; change customer-facing websites and support low-priority applications for individual departments. According to a IDC cloud research [1], worldwide revenue from public IT cloud services reached above $21.5 billion in 2010 and will reach $72.9 billion in 2015, representing a compound annual growth rate of 27.6%. These revenues imply that cloud computing is a promising platform. On the other hand, it enables the attackers to find the vulnerabilities in the model. Despite the potential benefits and revenues that could be gained from the cloud computing model, the model still has some open issues that instill fear among the enterprise IT community for adopting the cloud computing model fast. Vendor lock-in, multi-tenancy and isolation, data management, service portability, elasticity engines, SLA management, and cloud security are well known open research problems in the cloud computing model.

From the cloud consumers' perspective, security is the major concern that hampers the adoption of the cloud computing model because of the following facts

- Enterprises outsource security management to a third party that hosts their IT assets.
- Co-existence of assets of different tenants in the same location and using the same instance of the service while being unaware of the strength of security controls used.
- The lack of security guarantees in the SLAs between the cloud consumers and the cloud providers
- Hosting this set of valuables assets on publicly available infrastructure increases the probability of attacks.

2. CLOUD COMPUTING DEFINED

Before addressing the issues, it is important to understand what cloud computing means, the different types of cloud computing, and the various delivery mechanisms. The cloud model promotes seamless availability of computing resources (networks, servers, storage, applications and services) through shared pooling [3] and is defined in terms of 1) essential characteristics, 2) service models and 3) deployment models.

1) The Essential cloud characteristics are:

- On-demand self service
- Broad network access
- Resource pooling
- Location independence
- Rapid elasticity
- Measured service

2) The Cloud Service delivery Models are:

- Software as a Service (SaaS) – Access vendor application over internet
- Platform as a Service(PaaS)- Deploy customer-owned applications in a platform created by vendor in the cloud
- Infrastructure as a Service(IaaS)- Lease the processing environment, storage, network resources, and other fundamental computing resources

3) The cloud Deployment Models are:

Private cloud: Internally deployed and provisioned as in-house dynamic computing resources.

Community Cloud: shared infrastructure for specific community

Public cloud: sold to the public internet users. Deployed as mega-scale infrastructure

Hybrid cloud: composition of two or more cloud types.

3. CLOUD COMPUTING BENEFITS

3.1 Operational Efficiency

As computing becomes more and more pervasive with increasing adoption of smart devices, a new generation of application are required to manage the scale of information and processing economically. In order to increase the portfolio of offerings and to start innovation initiatives, business leaders turn to their IT departments to setup the information processing environment in short duration and budget. In today's world, customers, employees, and business partners live in their files and their files are their lives [3]. That means they want all of their data conveniently and reliably accessible no matter where or how it is stored, no matter what kind of application they are using to access files, and no matter what type of device is at their fingertips- a smartphone, a tablet, a laptop or a desktop. They want to be able to work and transact business anywhere, at any time. These demands cannot be met without efficient backend IT operations. Operational efficiency of cloud computing can be categorized in terms of financial, time and process.

Financial: Improved utilization and sharing of otherwise idle resources decreases the operational costs associated with the entire lifecycle of an application. It also reduces the capital expenses for IT projects as there is no upfront investment is required to purchase hardware and software assets.

Time: While often tightly coupled with financial considerations, the ability to rapidly provision resources can dramatically improve time-to-market, which, in turn, enables greater agility for both IT and business stakeholders in adapting to changing business conditions.

Process: Many operational efficiencies are "built in" to the processes required by IT and business stakeholders to deliver applications. The automation and orchestration of such processes affords organizations opportunities to evaluate those processes and eliminate unnecessary redundant, or otherwise disruptive steps. Cloud computing allows us to deploy the same service or topology of services repetitively. Automating repetitive tasks can mitigate the potential introduction of errors into those processes and reduce the time required to execute. And, in some cases, automation creates self-service opportunities that enhance the business stakeholder's desire for higher levels of control and visibility into IT processes.

3.2 Financial Benefits

Cost effective or cheap resources was the primary benefit associated with cloud computing. This is not hype. Sharing resources and the infrastructure needed to leverage those resources does, in fact, reduce costs to a level with which enterprise IT organizations cannot hope to compete. A cloud offering is a pay-as-you –go service, so there are no new capital expenditure for servers, storage systems, and VPN connections; there are no software upgrades and support costs; there is no need to hire and train new system administrators. Since most cloud services are easy to provision and deploy, with free trails and month-by-month terms available, businesses don't need to risk the expensive upfront investment typical hardware and software solutions require. The cloud services also typically works with a multitude of devices, scales on demand to accommodate growth or spikes in usage, and is accessible 24/7 virtually anywhere there is internet access.

Financial benefits associated with more rapid provisioning and a reduced time-to-market is also feasible within a private cloud-computing (enterprise-owned) implementation. By leveraging rapid provisioning and sharing of resources, IT organizations can respond more quickly to requests for resources-thus avoiding the lengthy acquisition and subsequent rollout processes required in traditional architectures. Because IT charges for most business projects based on time-which translates into costs-a reduction in time spent provisioning resources directly translates into financial savings for the project, as well as a shortened timeline to deploy.

The cloud model can also give companies the ability to leverage resources they already have- including both physical infrastructure such as servers and storage system as well as existing user credentials and security-related processes. This means IT can extract even more value from these resources by cloud-enabling them rather than force a "rip-and-replace" migration that increases risk and cost across the board.

3.3 Process Automation

Leveraging a private cloud also leads to repeatable deployments through automation, which can further decrease time-to-market and increase project completion and success rates. Repeatable deployments can be leveraged as "templates" to further provide a firm foundation upon which application deployment becomes a "service" that is more easily used by operators and business constituents alike. Faster time-to-market at every level increases competitive advantages and makes the business more responsive to its customers—an often incalculable benefit.

Automating deployments leads to greater use of resources primarily because automation requires integration and interaction across the entire delivery infrastructure. This level of collaboration enables finer-grained control by orchestration systems, which results in better use of resources and often in a more timely fashion. For example, automating scalability on demand for web applications requires proactive monitoring of usage, user performance, and capacity. Orchestration systems incorporate this data into decision-making processes that ultimately lead to faster capacity provisioning, which helps eliminate the degradation or disruption of service often associated with a manual provisioning process. Higher levels of responsiveness help business better meet service –level agreements for key performance indicators such as more efficient call center utilization or reduced customer abandonment rate.

4. CLOUD COMPUTING CHALLENGES

4.1 Security Management

Despite all the potential benefits, however, most businesses are still having concern in adopting cloud computing environment to host their key applications. The dominant concern is security. Business remains unsure whether their data is safe in the cloud, whether the cloud model has matured enough to address the myriad security issues it creates. I listed the three clouds service delivery models in section 2 and the relationship between these service models is depicted in figure 1. I will provide the analysis on the security and highlight the issues/vulnerabilities in each service delivery model in this section.

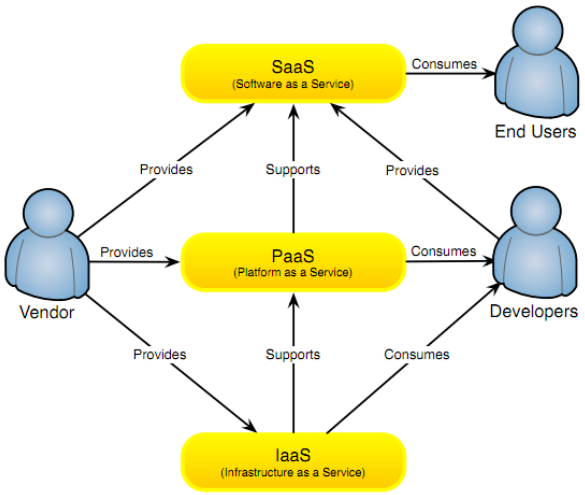


Figure 1: Cloud Computing Layer Interrelationships (source: Briscoe and Marinos [4])

4.1.1 IaaS Issues

IaaS (Infrastructure as services) are implemented through VMs (Virtual Machines). It remains a challenge to protect VM operating systems and workloads from common security threats that affect traditional physical servers, such as malware and viruses, using traditional or cloud-oriented security solutions.

VM security - The security of individual slice of VM is the responsibility of cloud consumer. Each cloud consumer can use their own security controls based on their needs, expected risk level, and their own security management process. Unlike physical servers VMs are still under risk even when they are offline. VM images can be compromised by injecting malicious codes in the VM file or even stole the VM file itself. Secured VM images repository is the responsibilities of the cloud providers.

Virtual network security – sharing of network infrastructure among different tenants within the same server (using vSwitch) or in the physical networks will increase the possibility to exploit vulnerabilities in DNS servers, DHCP, P protocol vulnerabilities.

Securing VM boundaries – VMs have virtual boundaries within main physical server platform. VMs that are deployed on the same server share the same CPU, Memory, I/O, NIC and other peripherals without any physical isolation. Securing VM boundaries is the responsibility of the cloud provider.

Hypervisor Security - hypervisor is a virtual machine manager that maps from physical resources to virtualized resources and vice versa. It is the main controller of any access to the physical server resources by VMs. Any compromise of the hypervisor violates the security of the VMs because all VMs operations become traced unencrypted. Hypervisor security is the responsibility of the cloud providers and the service provider. In this case, the service provider is the company that delivers the hypervisor software such as VMware or Xen.

4.1.2 PaaS Issues

PaaS model is based on the Service-oriented Architecture (SOA) model in the distributed environment. This leads to inheriting all security issues that exist in the SOA domain such as Impersonation, Phishing and social engineering, Brute force (dictionary) attacks, password reset attacks[6] etc. Authentication should be enforced through strict process like two-factor authentication such as smartcards or biometric mechanism. This security issue is a shared responsibility among cloud providers, service providers and consumers

PaaS may offer APIs that deliver management functions such as business functions, security functions, application management, etc. Such APIs should be provided with security controls and standards implemented such as OAuth framework [5], to enforce consistent authentication and authorization on calls to such APIs. Moreover, there is a need for the isolation of APIs in memory. This issue is under the responsibility of the cloud service provider.

4.1.3 SaaS Issues

SaaS provides access to software and its functions remotely as a Web-based service. In the SaaS model enforcing and maintaining security is a shared responsibility among the cloud providers and service providers (software vendors). The SaaS model inherits the security issues discussed in the previous two models as it is built on top of both of them. In addition to those issues, data locality, integrity, segregation, access, confidentiality, backups and network security are major concerns.

Web application vulnerability scanning – web applications to be hosted on the cloud infrastructure should be validated and scanned for vulnerabilities and attack paths maintained in the National Vulnerability Databases (NVD) [7] and the Common Weaknesses Enumeration(CWE) [8]]. Organizations should use single sign-on capabilities to access both the user's desktop and SaaS cloud services via single password. Web application firwalls should be in place to mitigate existing/discovered vulnerabilities. This will examine HTTP requests and responses for application specific vulnerabilities.

4.2 Vendor Risks

Vendors are taking significant responsibility of managing and protecting the customers' data and infrastructure. Instead of controlling the IT environment directly, through the implementation of technical specifications that they define, organizations have to manage their IT infrastructure through their relationship with the cloud providers and through service level agreements (SLAs).

Data Security: Verifying the vendor data handling processes along with the availability of data backup and the presence of other customers and service providers utilizing the same outsourced platform is extremely important before entering relationship with the vendor. A vendor without proper internal controls and regulatory standards may not be able to adequately secure the customer's data. Customers should request audit reports from the cloud vendor to manage the risk on more than 'vendor trust' alone. It is better to create a disaster recovery environment with different vendor for critical application to keep the application alive if the application environment goes down with primary vendor due to major outage.

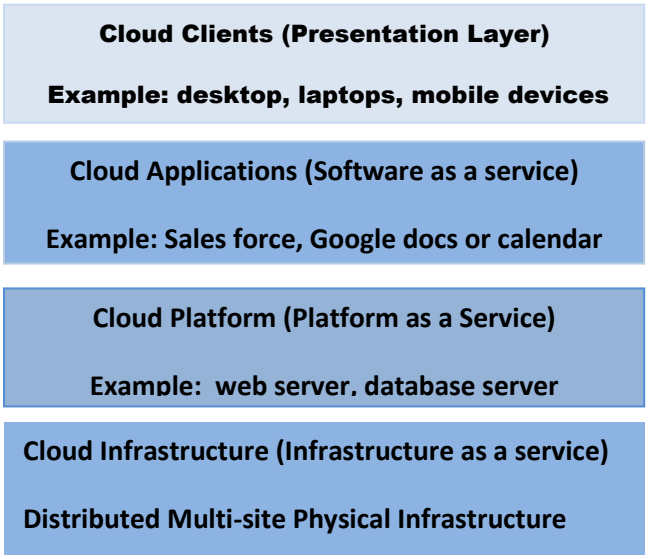
Vendor Disengagement: Disengagement of a vendor service is another complicated matter that should be considered during the planning stage and contract agreements should be specific to cover these details as to cleaning the data and dismantling the existing setup, ownership of data etc

Performance: . Poor application performance causes companies to lose customers, reduce employee productivity, and reduce bottom line revenue. Customers must make certain that application/infrastructure/platform performance is guaranteed by the vendor and performance parameters should bed in the SLA.

Transparency: Lack of transparency into infrastructure details that often come with moving to cloud services from traditional in-house infrastructure. Customers should manage vendors to meet services levels using SLAS. It will also take time for the organization staff to shift their skills from managing internal IT hosting environment to manage complex relationship with vendors

4.3 Layered cloud architecture

Cloud computing enables a decoupling of layers as depicted in figure 2, with both the customer and service provider taking on whatever level of value-added services with which they are most comfortable. In an increasing number of cases, the provider is itself the buyer of the other type of cloud service, such as a platform, infrastructure or physical rack space. PaaS service is not mostly used by end users today but a growing number of SaaS offerings are hosted within some other vendor's PaaS or IaaS.



Such a nested hosting arrangement increase the platform risks and especially the network risks associated with a multi-tenanted environment and it adds layers between the customer and the actual point of operations. This, combined with lack of transparency, increases the complexity and thus the security risks.

5. CONCLUSION

In a fast-paced global economy, today's IT organization want and need the resilience to quickly respond to business demands and market opportunities, and they need a cost-effective strategy for getting there. More and more IT managers are turning to cloud services to accelerate their responsiveness to business needs. Cloud services can enable faster time to market and reduced startup costs through faster IT deployments and end-user-self-service.

Despite the challenges explained in the above sections, benefits of moving the IT assets to cloud outweigh the challenges to be dealt after the migration. Cloud computing presents new challenges but the problems are familiar within the IT industry paradigm. Cloud providers need to work more to develop and tailor policies, procedures, standards and tools specifically to address the issues.

6. REFERENCES

[1] IDC revenue survey

http://www.idc.com/prodserv/idc_cloud.jsp.

[2] Peter Mell, and Timothy Grance

http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

[3] CIO white paper –IBM

http://www.ciosummits.com/media/pdf/cloud/IBM_staying_aloft_in_tough_times.pdf.

[4] Gerald Briscoe and Alexandros Marinos. "Digital Eco Systems in the Clouds: Towards Community Cloud computing," 2009,

http://arxiv.org/pdf/0903.0694v3

[5] OAuth 2.0 Framework

http://tools.ietf.org/html/draft-ietf-oauth-v2-31

[6] Security Considerations for Platform as a Service (PaaS) http://social.technet.microsoft.com/wiki/contents/articles/3809.security-considerations-for-platform-as-a-service-paas.aspx

[7] National vulnerability Database

http://web.nvd.nist.gov/view/vuln/search.

[8] Common weakness enumeration

http://cwe.mitre.org/.