International Journal of Emerging Engineering Research and Technology
Volume 5, Issue 2, February 2017, PP 32-35
ISSN 2349-4395 (Print) & ISSN 2349-4409 (Online)
DOI: http://dx.doi.org/10.22259/ijeert.0502004

My Cloud Data Logger

Lalitha Siva Jyothi Ballada

ABSTRACT

Cloud computing is the general term for the delivery of hosted services on the internet.

Cloud computing that enables companies to consume the compute resource, such as a virtual machine (VMs), storage or an application, as a utility -- just like the electricity -- rather than having to build and maintain the computing infrastructures in house which is built so far.

Cloud computing provides several attractive benefits for businesses and end users. Below three of the main benefits of cloud computing.

Self-service provisioning: End users can spin up to compute resources for all type of workloads on demand. This process can eliminate the traditional way need for IT administrators to provision, manage and use computer resources.

Elasticity: Companies can be scale up as computing needs increase and scale down again as per their demands decrease. This process eliminates the need for massive investments in the local infrastructure which may or may not remain active or useless.

Pay per use: The computer resources are measured at a high level, allowing users to pay only for the services and workloads which they use.

Keywords: Data Security Issues cloud, Cloud Security, Cloud Architecture, Cloud Data Protection

INTRODUCTION

Cloud Computing is the distributed architecture that ca concentrates server resources on the accessible platform to provide on demand computing resources and their services based on end user need. Cloud service a provider (CSP's) offers their cloud platforms for their customers to be use and to create their own web services; much like internet service providers offer their customers high speed broadband to access the internet. CSPs and ISPs (Internet Service Providers) for both offer services. Cloud computing is the model that enables convenient, on-demand network access to the shared pool of configurable computing resources like networks, servers, storage, applications that can be rapidly provisioned and released with minimal supervision effort or the service provider's interaction. In general cloud service provider's offers

Three types of services example- Software as a Service (SAAS), Platform as a Service (PAAS) and Infrastructure as a Service (IAAS).

There are several reasons for companies to move towards IT solutions that can be include cloud computing as they are just required to pay for the resources on usage basis. In addition, organizations can easily meet their needs of rapidly changing markets to ensure that they are always on the leading edge for their consumers. Cloud computing performed as a business necessity, being active by the idea of just consuming the infrastructure instead managing the infrastructure. Although initially this idea was present only in the academic area, recently, it was moved into industry by companies like Microsoft, Amazon, Google, Yahoo! and Salesforce.com. This makes it possible for new startup companies to enter the market easy way, since the cost of the infrastructure is greatly reduced. This process allows developers/programmers to concentrate on the business. The clients of commercial clouds rent computing power (virtual machines) or to storage allocation space (virtual space) dynamically, according to the needs of client business. With the activity of this technology, users can be access very heavy applications through lightweight portable devices like mobile phones, PCs.

Cloud computing is the new trend in the evolution of the distributed systems, the predecessor of cloud being the network. The user may not require knowledge or skill to control the infrastructure of the

clouds; it provides only abstraction. This can be utilized as a service of an Internet with very high scalability, higher throughput, quality of service and very high computing power. Cloud computing providers that deliver most common online business applications which are reliable and accessed from servers through web browser.

BENEFIS OF CLOUD COMPUTING

Flexibility: *The flexibility for enterprises is unprecedented. Enterprises could choose to outsource hardware while we maintaining control of their IT infrastructure; they can be completely-outsource all aspects of their infrastructure; or, often to driven by departmental advantages, enterprises are the deploying both completely and partially outsourced sections of their infrastructures as well.*

Cost Savings: *Infrastructure is on demand and leads to more efficient IT expenses. Restrictions on headcount and capital expenditures often hold back innovation. Regular demands point capacity requirements and require a strong infrastructure that is always underutilized. Cloud computing is a cost-effective alternative solutions.*

Mobility and Choice: *Technology is leading the development. Virtualization technologies like VMware enable applications and services to be moved from any internal environments to public clouds, or from one cloud service Providers to another provider.*

SCALABILITY

Infrastructure as a Service (IAAS) is equal with scalability. If there is an immediate need for servers, but if you have no time to complete capital acquisitions ? All you required is a credit card to get your infrastructure on demand. All departments and SMBs (including smaller service providers/MSPs) that need capacity on demand are controlled to take advantage of cloud computing. All types of disaster recovery and redundancy are also very high-impact to consume and leverage cloud computing.

SECURITY AND COMPLIANCE IN CLOUD COMPUTING

Considering virtual machines, which can contain critical applications and critical sensitive data for business, off premise to public and shared cloud environments arise security challenges for companies that have relied on the network perimeter protection as the main method to protect their datacenter. It could also revoke compliance and crack security policies. CIOs, recognizing that bigger competitive advantage, cost savings, expanded volume and failover flexibility are just too tempting to pass up, are looking at cloud computing.

CLOUD SECURITY CHALLENGES

At the first look, the security requirements for cloud computing providers would appear to be the same as old-style data centers apply a strong network security perimeter and retain the hackers out. However, as previously implemented, physical segregation and hardware-based security cannot defend against attacks between virtual machines on the same server that were hosted. For cloud computing providers to increase from the efficiencies of virtualization, virtual machines from multiple organizations should need to be co-located on the same physical resources. The below outlines some of the main concerns that enterprises should be also aware of when they planning their cloud computing deployments.

ADMINISTRATIVE ACCESS TO SERVERS AND APPLICATIONS

One of the big important features of cloud computing is that it offers "self-service" access to computing power, most likely through the Internet. In traditional datacenters, administrative access to the servers is controlled and limited to direct or on-premise contacts. In cloud computing, this administrative access should now be conducted through the Internet, growing exposure and risk. It is extremely important that to restrict the administrative access and should monitor that access to maintain brightness of changes in the system control.

DYNAMIC VIRTUAL MACHINES: VM STATE AND SPRAWL

Virtual machines are very dynamic. They can quickly be reverted to previous occurrences, paused and the restarted, fairly easily. They can also be willingly cloned and impeccably moved between the

physical servers. This dynamic nature and possible for VM sprawl makes it difficult to achieve and maintain consistent security. Vulnerabilities or configuration errors could be unknowingly broadcast. Also, it is difficult to maintain the auditable record of the security state of a virtual machine at any given Point in specific time of period. In cloud computing environments, it will be essential to be able to show the security state of a system, irrespective of its location or proximity to other, potentially uncertain virtual machines.

VULNERABILITY EXPLOITS AND VM-TO-VM ATTACKS

Cloud computing servers can use the same operating systems, enterprise and web applications as they localized virtual machines and physical servers. The skill for an attacker or malware to remotely adventure vulnerabilities in these systems and applications is the significant threat to virtualized cloud computing environments. In addition, co-location of many virtual machines raises the attack surface and risk of the VM-to-VM compromise. Interruption detection and prevention systems need to be able to notice malicious activity at the virtual-machine level, irrespective of the location of the VM within the virtualized cloud environment.

SECURING HIDDEN VIRTUAL MACHINES

Unlike the physical machine, when a virtual machine is offline, that is still available to use any application that can access the virtual machine that storage over the network, and is so vulnerable to malware infection. However, hidden or offline VMs could not have the skill to run an antimalware scan agent automatically. Dormant virtual machines may exist not just on the hypervisor but it can also be backed up or archived to other servers or storage media that can access. In cloud computing environments, the responsibility for the protection and scanning of dormant machines reposes with the cloud provider. Enterprises that using cloud computing should look for cloud service providers that can secure these types of dormant virtual machines and maintain solid security in the cloud.

PERFORMANCE IMPACT OF TRADITIONAL SECURITY

The existing content security solutions that were created prior to the concept of x86 virtualization and the cloud computing and that was not designed to operate in the cloud environments. In a cloud environment, where that virtual machines from one to different tenants share the hardware resources, synchronized full system scans can cause refreshing performance degradation on the important host machine. Cloud service providers providing the baseline of security for their hosting clients can be address this problem by performing the resource-intensive scans at the supervisor level to eliminating this contention at the host level.

THE PROPOSED SOLUTION FOR SECURITY

To avoid few security risks we have developed software "My Cloud Data logger" to know the client what is happening on the could server which bought from The cloud services this software is mainly deals with below modules.

1. Key Stroke Logger
2. Screen Shots Logger
3. Active Application Logger
4. Send an email to client about cloud server activity

1. Key Stroke Logger

In key stroke logger records every key stroke generated by the user and stored at the installation path in separate folder. It records all the keys that are operated in cloud server.

2. Screenshot Logger

This software takes the screen shots of the cloud server at the given interval of time supplied by the user. The image is stored as above in bmp format.

3. Active Application Logger

It captures each application name which runs on the system and recorded in the log file.

4. Send an Email to Client about Cloud Server Activity

My Cloud Data Logger software that we developed will intimate the client through email about their cloud server activity. Including logger and screenshots etc.

CONCLUSION

I believe if we follow the small tricks/ measures and using the software like "My Cloud Data Logger" We can better utilize the cloud services as cloud computing is the most popular notion in the IT today.

REFERENCES

[1] Kundu, C. D. Banerjee, P. Saha, "Introducing New Services in Cloud Computing Environment", International Journal of Digital Content Technology and its Applications, AICIT, Vol. 4, No. 5, pp. 143-152, 2010.

[2] Lizhe Wang, Jie Tao, Kunze M., Castellanos A.C., Kramer D., Karl W., "Scientific Cloud Computing: Early Definition and Experience," 10th IEEE Int. Conference on High Performance Computing and Communications, pp. 825-830, Dalian, China, Sep. 2008, ISBN: 978-0-7695-3352-0.

[3] R. L Grossman, "The Case for Cloud Computing," IT Professional, vol. 11(2), pp. 23-27, 2009, ISSN: 1520-9202.

[4] R. Kandukuri, R. Paturi V, A. Rakshit, "Cloud Security Issues", In Proceedings of IEEE International Conference on Services Computing, pp. 517-520, 2009.

[5] Meiko Jensen, JorgSchwenk, Nils Gruschka, Luigi Lo Iacon, "On technical Security Issues in Cloud Computing," Proc. of IEEE International Conference on Cloud Computing (CLOUD-II, 2009), pp. 109-116, India, 2009.

[6] Pringetal. "Forecast: Sizing the cloud; understanding the opportunities in cloud services," Gartner Inc., Tech. Rep. G00166525, March 2009.

[7] AmanBakshi, Yogesh B. Dujodwala, "Securing cloud from DDoS Attacks using Intrusion Detection System in Virtual Machine," ICCSN '10 Proceeding of the 2010 Second International Conference on Communication Software and networks, pp. 260-264, 2010, IEEE Computer Society, USA, 2010. ISBN: 978-0-7695-3961-4.