International Journal of Engineering Research and Applications (IJERA)
ISSN: 2248-9622 www.ijera.com
Vol. 2, Issue 2, Mar-Apr 2012, pp.451-456

Analysis of Cloud Computing Security Considerations for Infrastructure as a Service

INTRODUCTION I

Cloud computing is defined as the delivery of computing as a service rather than a product, whereby shared resources, software, and information are provided to computers and other devices as a metered service over a network (typically the Internet). Cloud computing is a marketing term for technologies that provide computation, software, data access, and storage services that do not require end-user knowledge of the physical location and configuration of the system that delivers the services. Cloud computing describes a new supplement, consumption, and delivery model for IT services based on Internet protocols, and it typically involves provisioning of dynamically scalable and often virtualized resources. It is a byproduct and consequence of the ease-of-access to remote computing sites provided by the Internet. This may take the form of web-based tools or applications that users can access and use through a web browser as if the programs were installed locally on their own computers. It provides deliver applications via the internet, which are accessed from web browsers and desktop and mobile apps, while the business software and data are stored on servers at a remote location. In some cases, legacy applications are delivered via a screen-sharing technology, while the computing resources are consolidated at a remote data center location. At the foundation of cloud computing is the broader concept of infrastructure convergence (or Converged Infrastructure) and shared services. This type of data center environment allows enterprises to get their applications up and running faster, with easier manageability and less maintenance, and enables IT to

more rapidly adjust IT resources (such as servers, storage, and networking) to meet fluctuating and unpredictable business demand. Most cloud computing infrastructures consist of services delivered through shared data-centers and appearing as a single point of access for consumers' computing needs. Commercial offerings may be required to meet service-level agreements (SLAs), but specific terms are less often negotiated by smaller companies.

The tremendous impact of cloud computing on business has prompted the federal United States government to look to the cloud as a means to reorganize their IT infrastructure and decrease their spending budgets. With the advent of the top government official mandating cloud adoption, many agencies already have at least one or more cloud systems online.

SECTION II

2.1. Features of Cloud Computing:

Cloud computing, as defined by the US National Institute of Science and Technology (NIST) includes the following features:

2.1.1.On-demand self-service. A user can obtain compute, network and storage capabilities without having to go through a mediator; this can be done through a self-service portal and requisition center of some type.

2.1.2 Broad network access. The information storage in the cloud infrastructure should be available from any location, and from a broad array of networked devices, such as desktops, laptops, PDAs, smart phones, and other devices that currently exist as well as those that will exist in the future.

2.1.3. Resource pooling. Compute, network and storage resources are delivered from a larger pool of resources and multiple tenants (different groups or organizations) take advantage of that same pool. There may also be location independence, as each tenant may or may not be aware of the location of particular resources at any point in time.

2.1.4. Rapid elasticity. Users can provision and deprovision resources quickly and easier. In addition, this provisioning and deprovisioning can be done automatically, based on policy, so that resources are assigned when required and released when they are no longer needed.

2.1.5. Measured Service. Users obtain compute, network and storage assets that they need, and pay for only those services that they use.

2.2. Architecture of Cloud computing

Cloud architecture is the systems architecture of the software systems involved in the delivery of cloud

computing, typically involves multiple cloud components communicating with each other over a loose coupling mechanism such as a messaging queue.

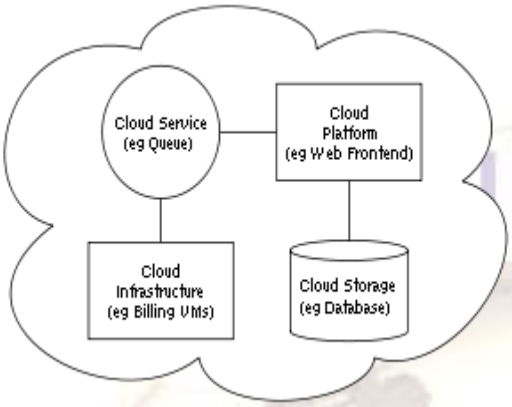

Figure 1 shows the platform of cloud computing.

2.2.1 Inter-cloud: The Intercloud is an interconnected global "cloud of cloudsand an extension of the Internet "network of networks" on which it is based.

2.2.2. Cloud engineering: Cloud engineering is the application of engineering disciplines to cloud computing. It brings a systematic approach to the high level concerns of commercialization, standardization, and governance in conceiving, developing, operating and maintaining cloud computing systems. It is a multidisciplinary method encompassing contributions from diverse areas such as systems, software, web, performance, information, security, platform, risk, and quality engineering. It Consists of four Layers. Once an internet protocol connection is established among several computers, it is possible to share services within any one of the following layers.

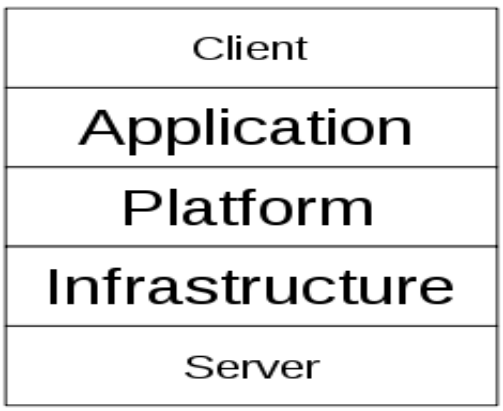

Figure 2. architecture of cloud computing

A. Client: A cloud client consists of computer hardware and/or computer software that relies on cloud computing for application delivery and that is in essence useless without it.

B. Application: Cloud application services or "Software as a Service (SaaS)" deliver software as a service over the Internet, eliminating the need to install and run the application on the customer's own computers and simplifying maintenance and support.

C. Platform: Cloud platform services, also known as platform as a service (PaaS), deliver a computing platform and/or solution stack as a service, often consuming cloud infrastructure and sustaining cloud applications.[37] It facilitates deployment of applications without the cost and complexity of buying and managing the underlying hardware and software layers. Cloud computing is becoming a major change in our industry, and one of the most important parts of this change is the shift of cloud platforms. Platforms let developers write certain applications that can run in the cloud, or even use services provided by the cloud.

There are different names being used for platforms which can include the on-demand platform, or Cloud 9. It's your choice on what you would like to call the platform, but they all have great potential in developing. When development teams create applications for the cloud, they must build its own cloud platform.

D. Infrastructure: Cloud infrastructure services, also known as "infrastructure as a service" (IaaS), deliver computer infrastructure – typically a platform virtualisation environment – as a service, along with raw (block) storage and networking. Rather than purchasing servers, software, data-center space or network equipment, clients instead buy those resources as a fully outsourced service. Suppliers typically bill such services on a utility computing basis; the amount of resources consumed (and therefore the cost) will typically reflect the level of activity.

The servers layer consists of computer hardware and/or computer software products that are specifically designed for the delivery of cloud services, including multi-core processors, cloud-specific operating systems and combined offerings.

International Journal of Engineering Research and Applications (IJERA)
ISSN: 2248-9622 www.ijera.com
Vol. 2, Issue 2, Mar-Apr 2012, pp.451-456

SECTION III

3. Cloud Models: There are two types of Cloud Models .They are cloud computing service Models and Cloud Deployment Models.

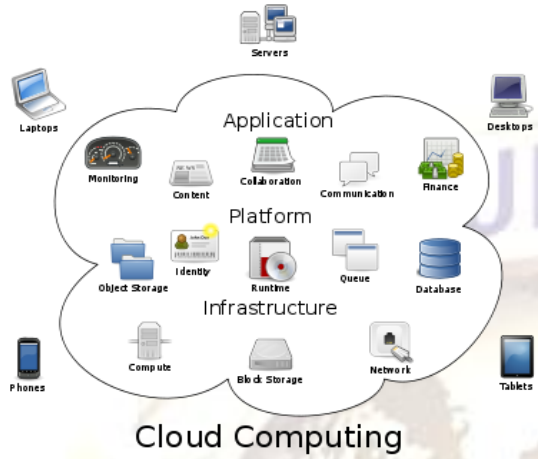

Figure 3. Infrastructure of cloud computing.

3.1. Cloud Service Models: Many people believe that cloud computing is just server virtualization, but cloud computing is much more than just server virtualization. Virtualization plays a huge role in cloud computing, and you can't have the cloud (at least not securely and cost effectively) without virtualization, but you can have virtualization without the cloud. Cloud computing is a delivery and consumption model, whereas virtualization is a technology that enables that model.
There are three service models for cloud computing:

3.1.1.Software as a Services (SaaS): With SaaS (also called "finished services"), users can rent applications that are ready to use. Overhead for acquisition is typically very low and commitments can be for short or long terms.

3.1.2. Platform as a Service (PaaS): PaaS, unlike SaaS, does not provide finished services to customers. Instead, PaaS provides a development platform that has built in cloud intelligence, so that developers don't need to worry about the underlying compute, network and storage infrastructure. All the developers need to do is develop the applications, using tools they already know how to use, and then deploy them to the PaaS provider. The PaaS provider's cloud engine then enables the core cloud competencies that are required for a cloud application, as noted in the first bulleted list above.

3.1.3. Infrastructure as a Service (IaaS): IaaS, in contrast to SaaS and PaaS, provides neither a finished service nor a development platform. Instead, IaaS provides the core compute, network and storage infrastructure on which you can build your own PaaS or SaaS environments. Essentially, IaaS provides an easy way for you to deploy virtualized servers in the cloud by taking advantage of server virtualization and automation.

3.2. Cloud Deployment Models: You also need to know about the cloud deployment models. The NIST identifies four deployment models .

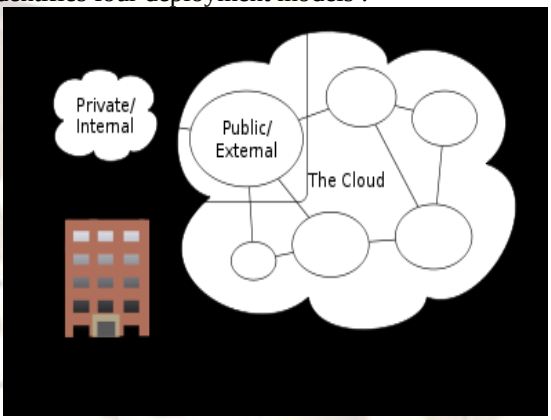

Figure 4 shows the deployment model of cloud computing.

3.2.1. Private cloud: A private cloud infrastructure is one where you control all the assets that participate in the cloud solution. The private cloud infrastructure might be located in your own datacenter, or it could be located in a hosted datacenter. Private cloud is infrastructure operated solely for a single organization, whether managed internally or by a third-party and hosted internally or externally. However, even located in the hosted datacenter, the private cloud is under your complete control – you control inbound and outbound access, you control the networking, you control the hardware and you control all of the software (operating systems an system services.)

3.2.2. Community cloud: A Community cloud shares infrastructure between several organizations from a specific community with common concerns (security, compliance, jurisdiction, etc.), whether managed internally or by a third-party and hosted internally or externally. The costs are spread over fewer users than a public cloud (but more than a private cloud), so only some of the benefits of cloud computing are realized .

3.2.3. Public cloud: In a public cloud, you rent services from the cloud provider. You might rent SaaS, PaaS or IaaS services, but you do not control all levels of the stack. In addition, public cloud environments are shared, multi-tenet environments, which mean that your services and data can be co-located with others, including competitors.

3.2.3. Hybrid cloud: Hybrid cloud is a deployment model where the organization takes advantage of both public and private cloud options. Hybrid cloud is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together, offering the benefits of multiple deployment models. It can also be defined as multiple cloud systems that are connected in a way that allows programs and data to be moved easily from one deployment system to another. For example, the firm might want to host a large array of web servers in the public cloud to be a customer front end for shopping and order taking, but then the private cloud is used to contain the customer and financial data that drive the transactions.

The deployment models are generally defined by who controls the cloud resources. The NIST document adds the "community cloud," in which multiple organizations come together to create a "semi-private" cloud. NIST further breaks the private and community cloud models into two sub-models: on-site and outsourced. The 84 page NIST document provides a good basis for understanding the basics of cloud computing.

3.3. Security in IAAS : Now that we have some basic definitions sorted out, let's focus on security in regard to Infrastructure as a Service or IaaS. Most administrators will be most comfortable and familiar with IaaS because it's very similar to what you're already doing now in your datacenter. Most likely, you have already deployed some kind of server consolidation plan to reduce the physical server footprint in your datacenter and save on energy costs. After server consolidation, you might then get interested in an IaaS offering, whereby you can take advantage of cloud features such as self-service and automation to help your company ramp up resources for application deployment and development faster than ever before. But before you do that, you'll need to think about the security implications of IaaS. The security issues are a little different, depending on whether you use a public cloud or private cloud implementation of IaaS. With a private cloud, your organization will have total control over the solution from top to bottom. With IaaS in the public cloud, you control the virtual machines and the services running on the VMs you create, but you do not control the underlying compute, network and storage infrastructure.

SECTION IV

4. Security performance of Cloud Computing

4.1. Data leakage protection and usage monitoring: Data stored in an IaaS infrastructure in both public and private clouds needs to be closely monitored. This is especially true when you're deploying IaaS in a public cloud. You need to know who is accessing the information, how the information was accessed (from what type of device), the location from which it was accessed (source IP address), and what happened to that information after it was accessed (was it forwarded to another user or copied to another site). You can solve these problems by using modern Rights Management services and applying restrictions to all information that is considered business critical. Create policies for this information and then deploy those policies in a way that doesn't require user intervention (don't make it the user's responsibility to decide which information is business critical and should be rights-protected). In addition, you should create a transparent process that controls who can see that information and then create a "self-destruct" policy for sensitive information that does not need to live indefinitely outside of the confines of the corporate datacenter.

4.2. Authentication and authorization

In order to have an effective Data Loss Prevention (DLP) solution – we need to have robust authentication and authorization methods in place. We can all agree that user name and password is not the most secure authentication mechanism. Consider two factor or multi-factor authentication for all information that needs to be restricted. In addition, consider tiering your access policies based on the level of trust you have for each identity provider for your IaaS cloud solutions. The level of authorization you enable from an identity provide such as Google Mail is going be a lot lower than if the identity provider is your corporate Active Directory environment. Integrate this authorization tiering into your DLP solution.

4.3. End to end logging and reporting

The effective deployment of IaaS, both in the private and the public cloud, demands that you have comprehensive logging and reporting in place. As

virtual machines are spun up automatically and moved between servers in an array dynamically over time, you never know where your information might live at any place in time (and this becomes even more interesting when we look at the issue of storage virtualization and dynamic migration). In order to keep track of where the information is, who accesses it, which machines are handing it, and which storage arrays are responsible for it, you need robust logging and reporting solutions.

The logging and reporting solutions are important for service management and optimization, and they will become even more important in the event of a security breach. Logging is critical for incident response and forensics – and the reports and findings after the incident are going to depend heavily on your logging infrastructure. Make sure that all compute, network, memory and storage activity is logged and that the logs are stored in multiple, secure locations with extremely limited access. Ensure that the principle of least privilege drives your log creation and management activities.

4.4. Infrastructure hardening

You need to make sure that your "golden image" virtual machines and VM templates are hardened and clean. This can be done with initial system hardening when you create the images, and you can also take advantage of technologies that enable you to update the images offline with the latest service and security updates. Make sure that you have a process in place to test the security of these master images on a regular basis to confirm that there has been no drift from your desired configuration, either due to malicious or non-malicious changes from the original configuration.

4.5. End to end encryption

IaaS as a service, both in public and private clouds, needs to take advantage of encryption from end-to-end. Make sure that you use whole disk encryption, which ensures that all data on the disk, not just user data files, are encrypted. This also prevents offline attacks. In addition to whole disk encryption, make sure that all communications to host operating systems and virtual machines in the IaaS infrastructure are encrypted. This can be done over SSL/TLS or IPsec. This includes not only communications from management stations, but also communications between the virtual machines themselves (assuming that you allow communications between the virtual machines). Also, when available, deploy mechanisms such as homomorphic encryption to keep end-user communications safe and secure. This is a form of encryption that allows complex calculations to be performed on the data even though it is encrypted.

CONCLUSION V

Cloud computing brings many great changes to traditional IT architectures. Those changes are diametric to some security precautions. Current cloud computing systems have unreliable security assurances. Security professionals need to prepare to support internal and external clients. Cloud computing is still struggling in its infancy, with positive and negative comments made on its possible implementation for a large-sized enterprise. IT technicians are spearheading the challenge, while academia is bit slower to react. Several groups have recently been formed, such as the Cloud Security Alliance or the Open Cloud Consortium, with the goal of exploring the possibilities offered by cloud computing and to establish a common language among different providers. In this boiling pot, cloud computing is facing several issues in gaining recognition for its merits. Its security deficiencies and benefits need to be carefully weighed before making a decision to implement it. However, the future looks less cloudy as far as more people being attracted by the topic and pursuing research to improve on its drawbacks. Our work extends with the Cloud platforms become ubiquitous, we expect the need for internetworking them to create market-oriented global Cloud exchanges for trading services. Several challenges need to be addressed to realize this vision. They include: market-maker for bringing service providers and consumers; market registry for publishing and discovering Cloud service providers and their services; clearing houses and brokers for mapping service requests to providers who can meet QoS expectations; and payment management and accounting infrastructure for trading services. Finally, we need to address regulatory and legal issues, which go beyond technical issues. Some of these issues are explored in related paradigms such as Grids and service-oriented computing systems. Hence, rather than competing, these past developments need to be leveraged for advancing Cloud computing. Also, Cloud computing and other related paradigms need to converge so as to produce unified and interoperable platforms for delivering IT services as the 5th utility to individuals, organizations, and corporations.

References

[1] L. Kleinrock. A vision for the Internet. *ST Journal of Research*, 2(1):4-5, Nov. 2008.
[2] S. London. INSIDE TRACK: The high-tech rebels. *Financial Times*, 6 Sept. 2008.
[3] I. Foster and C. Kesselman (eds). *The Grid: Blueprint for a Future Computing Infrastructure*. Morgan Kaufmann, San Francisco, USA, 2009.
[4] M. Chetty and R. Buyya. Weaving Computational Grids: How Analogous Are They with Electrical Grids? *Computing in Science and Engineering*, 4(4):61-71, July-Aug. 2008
[5] D. S. Milojicic, V. Kalogeraki, R. Lukose, K. Nagaraja, J. Pruyne, B. Richard, S. Rollins, and Z. Xu. Peer-to-Peer Computing. Technical Report HPL-2002-57R1, HP Laboratories, Palo Alto, USA, 3 July 2007
[6] D. Abramson, R. Buyya, and J. Giddy. A Computational Economy for Grid Computing and its Implementation in the Nimrod-G Resource Broker, *Future Generation Computer Systems*, 18(8):1061-1074,Oct. 2002.
[7] A. Weiss. Computing in the Clouds. *netWorker*, 11(4):16-25, Dec. 2007.
[8] Twenty Experts Define Cloud Computing. http://cloudcomputing.sys-con.com/read/612375_p.htm [18 July 2008].

N.Sainath working as Associate Professor in the department of IT, Sree visvesyaraya institute of science and technology .he is having 7 years of teaching experience and has involved in research work in the area of Networksecurity , mining , sensor networks , software engineering. etc. He is also involved in guiding several M.Tech and B.Tech IEEE Projects. He is enrolled for memberships such as IEEE , CSI , ISTE.

Vikram Narayandas working as Associate Professor in the department of CSE, Jayaprakash Narayan College Of Engineering .he is having 6 years of teaching experience and has involved in research work in the area of networksecurity , mining, sensor networks , software engineering. etc. He is also involved in guiding several M.Tech and B.Tech IEEE Projects.

S.Jayakrishna working as professor in the department of Management Studies , Sree visvesyaraya institute of science and technology .he is having 12.5 years of teaching experience and has involved in research work in the area of networksecurity , mining , sensor networks , software engineering. etc. Qualification is B.Tech (Mechanical), M.Tech(Production),),M.Tech(cse), MBA.memberships are MISTE , MIAPQR.

N. Aravind Kumar pusuing M.Tech having 3 years of Academic Experience, currently he is working as Asst prof at Sree Visvesyaraya Institute of science & Technology. His research areas include Data Mining, Networks, Software Engineering.