INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

A Review on Security Issues in Internal Cloud

Rupandeep Virk[1], Taranpreet Kaur [2]

[1, 2] Student
Lovely Professional University
Phagwara, Pin no. **144806**
[1]rupanvirk90@gmail.com,
[2]taranbhatia73@gmail.com

Abstract: *The concept of cloud computing is a very vast Concept. Cloud computing being an emerging technology has attracted more attention, as a result more and more enterprises have started to explore cloud computing. But besides these potential gains, the organizations are slow in accepting it due to security issues and challenges associated with it. With the extensive use of cloud computing, security issues came out on a growing scale and have become one of the major issues which hamper the growth of cloud. So, it has become necessary to solve these security issues to promote the wider applications of cloud computing.*

Keywords: *Cloud, Internal Cloud, Private cloud.*

1. INTRODUCTION

Cloud computing is the use of computing resources like hardware and software which are delivered over a network like internet as a service.

Cloud Computing refers to both the applications delivered as services over the Internet and the hardware and systems software in the datacenters that provide those services. The US National Institute of Standards and Technology (NIST) define cloud computing as "a model for user convenience, on demand network access contribute the computing resources (e.g. networks, storage, applications, servers, and services) that can be rapidly implemented with minimal management effort or service provider interference" With the rapid change in computer technology cloud computing has gained much attention which will bring changes in the IT industry, but along with that it leads to some security challenges. Security has become restriction in the development of cloud computing. So security issues need to be resolved. [3, 8]

.

2. CLOUD: OVERVIEW

2.1. Service models

There are three service models:-[5]

Cloud Software as a Service (SaaS): The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser. (e.g., web-based email)

Cloud Platform as a Service (PaaS): The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider.

Cloud Infrastructure as a Service (IaaS): The capability provided to the consumer is the provision of computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications.(e.g., host fire walls)

2.2. Cloud Deployment Models

There are four cloud deployment models:-[7]

Public Cloud: The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.

Private Cloud: The cloud infrastructure is operated solely for a single organization. It may be managed by the organization or a third party, and may exist on-premises or off premises.

Community Cloud: The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, or compliance considerations).

Hybrid Cloud: The cloud infrastructure is a composition of two or more clouds (private, community, or public). . In a hybrid cloud, a company can leverage third-party cloud providers in either a full or partial manner. This increases the flexibility of computing. The hybrid cloud environment is also capable of providing on-demand, externally-provisioned scalability. Augmenting a traditional private cloud with the resources of a public cloud can be used to manage any unexpected rise in workload.

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

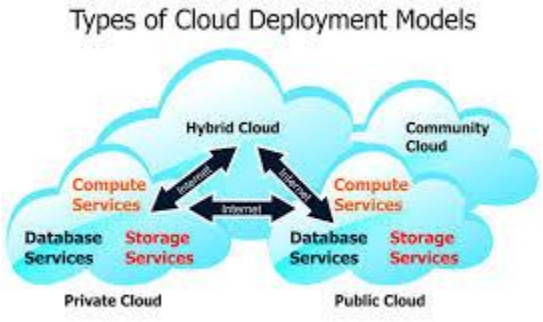

Figure 1: Types of Cloud Deployment Models [6]

2.3. Internal cloud as a part of private cloud

Private clouds are those that are built exclusively for an individual enterprise. They allow the firm to host applications in the cloud, while addressing concerns regarding data security and control, which is often lacking in a public cloud environment. There are two variations of private clouds:

On-Premise Private Cloud: This format, also known as an "internal cloud," is hosted within an organization's own data center. It provides a more standardized process and protection, but is often limited in size and scalability. Also, a firm's IT department would incur the capital and operational costs for the physical resources with this model. On-premise private clouds are best used for applications that require complete control and configurability of the infrastructure and security.

Externally-Hosted Private Cloud: This private cloud model is hosted by an external cloud computing provider. The service provider facilitates an exclusive cloud environment with full guarantee of privacy. This format is recommended for organizations that prefer not to use a public cloud infrastructure due to the risks associated with the sharing of physical resources. Internal and external. Internal cloud is hosted within an organization's own data center. It provides a more standardized process and protection, but is often limited in size and scalability. Also, a firm's IT department would incur the capital and operational costs for the physical resources with this model. On-premise private clouds are best used for applications that require complete control and configurability of the infrastructure and security. External private cloud model is hosted by an external cloud computing provider.

Oracle has released a set of infrastructure-as-a-service (IaaS) systems that allows customers to use cloud computing features such as capacity on demand within the security and control of their in-house datacenter. Oracle IaaS, the on-premise, private cloud infrastructure is available for a monthly fee and can be used to deploy fully-integrated engineered systems

3. EIGHT KEY INGREDIENTS FOR BUILDING AN INTERNAL CLOUD

There are eight key ingredients to consider when building an internal compute cloud: [1]

3.1. Shared Infrastructure.

IT staff needs to understand how to configure the underlying storage and networking so that when it is brought together it can be shared across all of the enterprise's different workloads

3.2. Self-Service Automated Portal.

It is essential to make sure that the compute cloud can be consumed in an easy form by both developers and IT professionals. There is a need for self-service capabilities, and for highly automated provisioning portals that provide the ability to add workloads without having to go through all of the many different steps of provisioning with the network and underlying storage.

3.3. Scalable.

An effective cloud solution has to be scalable. IT organizations should think about boundary conditions in a more creative way, instead using the traditional models of scalability. As a new workload request comes up, they must determine where to provision that specific workload.

3.4. Rich Application Container.

Clouds need to have a richer application container that will show the different interdependencies between components of the application, specifically those that take place between different virtual machines. This information helps create the correct network subnets so that the storage will work well together and not be isolated from one another.

3.5. Programmatic Control.

It is very common for a compute cloud to have programmatic control.

3.6. 100% Virtual Hardware Abstraction. Clouds need 100% hardware abstraction. This can include servers or other physical devices like storage. In a cloud environment, the user should be able to interact with the virtual machines and other devices through the user interface, verses actually changing physical infrastructure.

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

3.7. Strong Multi-Tenancy.

Strong multi-tenancy involves extensive use of VLANs to isolate network traffic between different zones in the cloud. This is a common requirement in internal clouds, to make sure that authorized users have access to certain applications.

3.8. Chargeback.

IT organizations must be able to create effective and accurate chargeback capabilities. For internal clouds, even if funds aren't literally exchanged,, the ability to create transparency in costs and services can help justify expenses.

4. SECURITY ISSUES IN INTERNAL CLOUD [2, 4, 9]

4.1. Internal Private cloud computing security: Comingled regulatory environments

In an internal just because an infrastructure is dedicated to your use alone, everything can't go there with equal ease. Even if private internal cloud assures greater control over security still regulatory compliance should be there particularly when multiple types of regulated data are in play, such as a comingled mix of payment card data, sensitive business intelligence and customer data. . Security professionals know not every IT environment fits every situation.

4.2. Data Expansion

Cloud supports resource centralization. For example, a virtualized environment can allow far-flung resources to come together under one environment. However, with the centralization of resources, data becomes "denser." It is beneficial for management, but it can become challenging from a security point, particularly when considering tools that operate across that data in aggregate. Bulk encryption, antimalware scanning and data "discovery" tools will face great difficulty dealing with very large amounts of data. Existing tools should be examined to determine how they will be impacted as data volumes increase.

4.3. Defining responsibilities

In case of public cloud, quite a bit of energy goes to define who does what, when and how. In an internal private cloud deployment, responsibility for operational aspects of security may change hands too from one group to another or to a service provider. Here also defining who is responsible for what and defining minimum levels of service is just as important. This is particularly true when security controls are close to end users -- i.e., when business owners responsible for applications/services have informal arrangements with groups that maintain infrastructure technically. But when responsibilities are to be exchanged, care should be taken to formalize existing arrangements.

4.4. Future Proofing

The defining aspect of private cloud is about who uses the infrastructure, not who maintains it. Even if a deployment uses dedicated resources today, it won't prevent it from migrating off-premises onto shared infrastructure tomorrow. Organizations adopting private infrastructure should know that what they today put into a private environment could easily migrate tomorrow.

4.5. Virtualization security issue.

Internal clouds have virtualization security issues similar to those of public clouds. The security of virtual infrastructure remains a top concern for enterprises.

4.5.1. Zoning: By providing virtual switches that allow communication between guests on a physical host, virtualization hides a considerable amount of traffic from traditional physical network protection – this includes intrusion detection and intrusion prevention systems (IDSs/IPSs).

4.5.2. Privileged administrators: Virtualization creates administrators whose power is greater than that of Windows Administrator. Most organizations tackle this issue by increasing monitoring and enhancing procedural controls, but several third-party products are emerging to enforce segregation of duties among computer, network, and storage and security roles in virtual environments.

4.5.3. Configuration and patch management: Virtualization creates a new layer of software that must be managed in accordance with change control procedures, patched periodically and protected from attack.

4.6. Viability of security tools

When an organization "virtualizes" a physical host (i.e. moves it from dedicated hardware to a virtual image), it always needs to evaluate how network-aware tools will be impacted. Any tool that presupposes visibility into traffic may be impacted: network IDS, traffic monitors and sniffers. For example, consider an n-tier Web application with separate Web, application and DB servers attached to one switch that's monitored by an ID. If those three devices are moved to virtual slices on a hypervisor, traffic is no longer visible on the wire, causing the IDS to lose visibility. This is a known issue in public deployments, but often is given less scrutiny

in a private scenario. Unless the organization plans accordingly, for example by deploying a "virtual tap" or configuring the hypervisor to offload traffic, existing tools may stop working. This is particularly true when large numbers of hosts are virtualized at one time; more hosts (typically) mean less time spent planning per host. However, creating a more "cloudy" internal virtual infrastructure has its own potential problems:

4.6.1. Server sprawl: If users are allowed to create new systems through a self-service provisioning portal, how do you ensure they don't sprawl?

4.6.2. Multi-tenancy: As different business units create their own systems, can you be sure that "tenants" are properly separated and controlled?

4.6.3. Governance models: Who is ultimately responsible for the virtual infrastructure – central IT or the departments that request virtual resources?

5. SUMMARY

Cloud Computing is the fundamental change happening in the field of Information Technology. [10] Cloud computing is providing enterprises with a fundamentally new way to cost-effectively and quickly deploy services and capabilities. Security of data is the main issue in a private cloud. Apart from security, there are other issues such as reliability, performance etc. In the private cloud, there are security concerns on data protection, proper segregation of data, proper logging and auditing. However, there are new securities issues arise due to the use of virtualization technologies. Issues such as network segmentation, firewalling, hypervisor integrity are all net new compared to traditional data centers. So in order to get the best use of cloud computing applications we need to resolve these security issues.

REFERENCES

[1] **Eight Key Ingredients to Building An Internal Cloud, source- V M Ware, 2009, type-white paper.**

[2] **F. A. Alvi, B. S Choudary2, N. Jaferry 3E. Pathan, A review on cloud computing security issues & challenges.**

[3] **Michael Armbrust, Armando, Fox, Rean Griffith, Anthony D. Joseph, Randy H. Katz, Andrew Konwinski, Gunho Lee, David A. Patterson, Ariel Rabkin, Ion Stoica, Matei Zaharia, Above the Clouds: A Berkeley View of Cloud Computing, February 2009.**

[4] **Balachandra Reddy Kandukuri, Ramakrishna Paturi V, Dr Atanu Rakshit , Cloud security issues, IEEE International Conference On Services Computing, 2009**

[5] **http://www.dummies.com/how to/content/ cloud-computing-models.html**

[6] **https://www.google.co.in/search?q=cloud+deployment+models**

[7] **http://www.cloud-competencecenter.com /understanding/cloud-computing-deployment-models/**

[8] **www.amazon.com/CloudComputing-Practica l -Introduction-Issues/dp/0580703223**

[9] **searchcloudsecurity.techtarget.com/tip/Cloud-computing-security-Infrastructure - issues.**

[10] **Study on Cloud Computing Security, Journal of software, FENG Deng-Guo,ZHANG Min+,ZHANG Yan,XU Zhen**