CLOUD COMPUTING PHYSICAL SAFETY MEASURES IN CLOUD ARCHITECTURE

Indravadan S. Patel*

Sonal J. Patel*

ABSTRACT

Cloud Commuting are multi tier application that provide the facility to end user without installing any software, server and database for using any web based application except live internet connection and any compatible browser. Cloud computing provides web based solution to end user, business user or any organization globally solution and access from anywhere as per their rights. This may take the form of web-based tools or applications that users can access and use through a web browser. A part from cloud environments or architecture based web solution there are used different types of hardware with high configuration for application server, database server, load balancer, cloud data centre, networking devices and many more. For the advancement of the end user facility all the business logic and data are stored at one place either it is form of private, public or hybrid cloud. So there are some physical safety aspect of challenges like short circuit, building collapse, theft of hardware, espionage, hardware failure, backup, fire and etc.

Keywords: *Cloud technologies, Cloud computing architecture, Cloud Computing Security.*

*Assistant Professor, Department of Computer Science, Ganpat University, Mehsana, Gujarat, India.

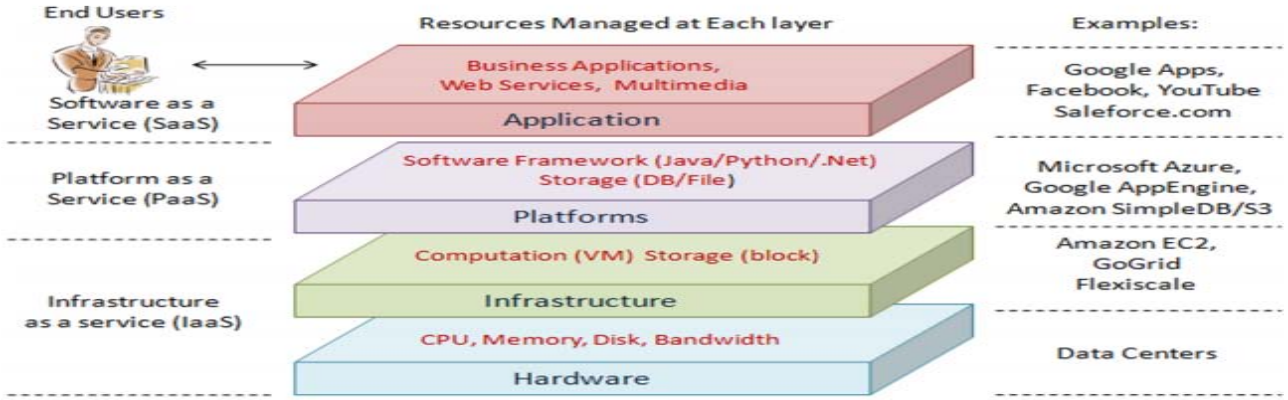
1. INTRODUCTION

Though there is no official definition and straight forward way to explain what exactly cloud computing is, but it can be expressed in general as the statement: “cloud computing is such a type of computing environment, where business owners outsource their computing needs including application software services to a third party and when they need to use the computing power or employees need to use the application resources like database, emails etc., they access the resources via Internet”.

For instance, you have a small business, where you need a few small servers for database, emails, applications etc. Normally, servers need higher computing power. On the other hand, PCs or laptop needs lower computing powers and are much cheaper than servers. Moreover, to maintain a client-server environment you need to have a highly skilled network maintenance team. If you decide to avoid the need of purchasing servers and thus cut-off the need of keeping an operation and maintenance team, then going for clouding computing is a very cost-effective solutions. Because in a cloud architecture, you neither have to install nor maintain servers. Just by paying a fixed amount of monthly charge you can outsource your IT infrastructure into a third party IT managed service data center [1].

2. CLOUD COMPUTING SERVICE MODEL

Fig 1: Cloud Computing Architecture



Cloud Infrastructure as a Service (IaaS). The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls).

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. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but does control the deployed applications and possibly application hosting environment configurations.

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). The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings [2].

3. INFRASTRUCTURE MODEL

There are four categories of cloud currently in the marketplace or emerging in the near future: public clouds, private clouds, virtual private clouds, and eventually inter-clouds.

Public Clouds: Public clouds are "stand-alone," or proprietary, clouds mostly off-premise, run by third party companies such as Google, Amazon, Microsoft, and others. Public clouds are hosted off customer premises and usually mix applications (transparently) from different consumers on shared infrastructure.

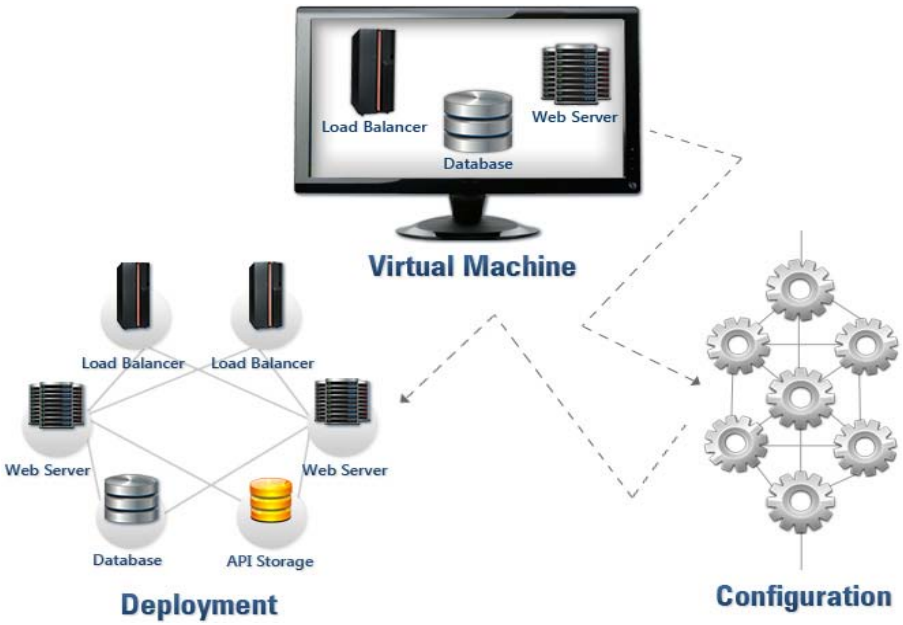
Private Clouds: Private clouds are typically designed and managed by an IT department within an organization. A private cloud is usually built specifically to provide services internally to an organization. Private clouds may be in a collocated facility or in an existing data centre. This model gives a high level of control over the cloud services and the cloud infrastructure.

Virtual Private Clouds: Virtual private clouds allow service providers to offer unique services to private cloud users. These services allow customers to consume infrastructure services as part of their private clouds. The ability to augment a private cloud, with on-demand and at-scale characteristics, is typical of a virtual private cloud infrastructure. Private cloud customers can seamlessly extend the trust boundaries (security, control, service-level management, and compliance) to include virtual private clouds. The virtual private cloud concept introduces the complexities of migrating workloads and related data from a private cloud.

Inter-cloud: The inter-cloud will emerge as a public, open, and decoupled cloud-computing internetwork, much like the Internet. In a sense, the inter-cloud would be an enhancement and extension of the Internet itself. Just as the Internet decouples clients from content (i.e., you don't have to have a pre existing agreement with a content provider to find and access its website in real time), the inter-cloud will decouple resource consumers (enterprises) from cloud resource providers, allowing the enterprises to find resources on demand with providers. Workload migration will be the dominant use case for the inter-cloud, as an open market, establishes trust standards and public subsystems for naming, discovering, and addressing portability and data/workload exchange [3].

4. HARDWARE USES IN ARCHITECTURE

Fig 2: Hardware Uses in Architecture



As per the figure 2 there are different types of hardware are used for request processing like server management, data base management, load balancing, network switches, network router, application server, database server, lots of cabling environment.

4. PHYSICAL SAFETY MESURES

Fig 3: Typical Server room

As the above figure indicate that there are lots of server are used in any data centre or cloud computing architecture. In any type of cloud computing architecture either it is public or private or any other there are different kind of hardware are used like lots of cabling, server machine, router machine, load balancer, and power supply devices. As per the above details there are many chance of risk like:

- Short Circuit
- Hardware Theft
- Building Safety from Fire
- Building Construction
- Sabotage
- Espionage

Short Circuit: Due to high volume of server capabilities and connection of different hardware with high voltage of power there are different cabling are used. Due to the overload of voltage supply or badly managed cable there are chance of short circuit. And this short circuit will create the fire and it may be create major hazard in the server building.

Fig 4: Cabling Diagram in Server Room

Hardware Theft: Cloud Architecture consists of lots of server and hardware so to manage the all the system successfully there are different skilled person are involved. There may be chance of hardware theft due to insider employee of outside person. And this hardware contains the lots of storage capabilities as well as end user storage data and some application code also.

Building Safety from Fire: There is different kind of hazardous possibilities after using lots of power usage, cabling, server capabilities. So there is lots of chance of fire. In that there must be set up as per the fire protection standard [4].

Building Construction: Building construction should be as per the standard and it can resist from earthquake, it can be tackle from high wind speed means hurricane or tornado, the server room is not stores at the top floor of the building [5].

Sabotage/Espionage: In the Cloud architecture may have lots of employees are working inside the department. So there are chance to breach of their important implementation and deployment details of cloud architecture and data of end user as well as some important cloud software.

5. CONCLUSION

While Security emerges as a major concern among those who respond to cloud computing surveys, the key to understanding security in cloud computing is not hacking the system but also considering the physical security like fire, earthquake, sabotage and many more hardware related risk. So it would also be consider while designing or implementing any cloud architecture.

6. REFERENCES

[1] Cloud Computing Architecture http://andromida.hubpages.com/hub/cloud-computing-architecture

[2] Cloud Computing Security, A Trend Micro White Paper, May 2010

[3] Cisco Cloud Computing - Data Center Strategy, Architecture and Solutions. – White Paper 1st Edition.

[4] List of NFPA Codes & Standards http://www.nfpa.org/aboutthecodes/list_of_codes_and_standards.asp

[5] Earthquake Resistant Design of Structures- http://www.bis.org.in/other/quake.htm#