3rd International Conference on Emerging Trends in Engineering and Management Research
Institution of Electronics and Telecommunication Engineers, IETE Indiranagar, Pune, India (ICETEMR-17)
30th July 2017, www.conferenceworld.in ISBN: 978-93-86171-55-9

CLOUD COMPUTING-ISSUES AND CHALLENGES

Asstt. Prof.Vandana

S.D.S.P.Memorial College for Women, Rayya (India)

ABSTRACT

Cloud computing is a multifaceted technological paradigm that is outgrowth of decades of research in parallel computing, virtualization, networking and communication, utility computing and Service-Oriented Architecture. It offers the facility to access shared resources and common infrastructure. It offers an innovative business model for an organization to adopt IT services. Every technology comes with a baggage of some pros and cons. Similarly, cloud computing too comes with its share of issues and challenges despite being core strength of some business industries. It also can create some major problems under some rare circumstances. Issues and challenges of cloud computing are characterized as ghosts in the cloud. This work presents an overview, style and models of cloud computing with the objective of presenting challenging issues concerned with various aspects of cloud computing.

I. INTRODUCTION

Cloud computing is "An emerging computer paradigm where data and services reside in massively scalable data centers in the cloud and can be accessed from any connected devices over the internet" A cloud is a virtualized server pool which can provide the different computing resources of their clients. Cloudcomputingmeans using multi-server computers via digitalnetwork, as though they were one computer.It is new computing paradigm involving data or computation outsourcing with-

- Infinite & elastic resource scalability.
- On demand "Just in time" provisioning.
- An upfront cost... Pay-as-you-go.

II. ESSENTIALELEMENTS

Thus, the**essential elements** of cloud computing is clearly articulated:

2.1. On-demand self-service

A consumer with an instantaneous need at a particular timeslot can avail computing resources (such as CPU time, network storage, software use, and so forth) in an automatic (i.e. convenient, self-serve) fashion without resorting to human interactions with providers of these resources.

2.2. Broad network access

These computing resources are delivered over the network (e.g. Internet) and used by various client applications with heterogeneous platforms (such as mobile phones, laptops, and PDAs) situated at a consumer's site.

2.3. Resource pooling

A cloud service provider's computing resources are 'pooled' together in an effort to serve multiple consumers using either the multi-tenancy or the virtualization model, "with different physical and virtual resources dynamically assigned and reassigned according to consumer demand".

2.4. Rapid elasticity

For consumers, computing resources become immediate rather than persistent: there are no up-front commitment and contract as they can use them to scale up whenever they want, and release them once they finish to scale down. Moreover, resources provisioning appears to be infinite to them, the consumption can rapidly rise in order to meet peak requirement at any time.

2.5. Measured Service

Although computing resources are pooled and shared by multiple consumers (i.e. multi-tenancy), the cloud infrastructure is able to use appropriate mechanisms while retaining privacy & security over their information.

2.6. Everything as service

In the cloud computing, everything is provided as a service like software as a service (SaaS), Platform as a service (PaaS), Hardware infrastructure as a service (HaaS), Security as a service (SaaS), Data as a service (DaaS).

III. SERVICE MODEL

In addition to these essential characteristics, the cloud community has extensively used the following service models to categories the cloud services:

- **Software as a Service (SaaS).** Cloud consumers release their applications on a hosting environment, which can be accessed through networks from various clients (e.g. web browser, PDA, etc.) by application users. Cloud consumers do not have control over the Cloud infrastructure that often employs E.g. - Google Mail, Google Docs, and so forth.
- **Platform as a Service (PaaS).** PaaS is a development platform supporting the full "Software Lifecycle" which allows cloud consumers to develop cloud services and applications (e.g. SaaS) directly on the PaaS cloud. E.g.- Google AppEngine.
- **Infrastructure as a Service (IaaS).** Cloud consumers directly use IT infrastructures (processing, storage, networks, and other fundamental computing resources) provided in the IaaS cloud. Virtualization is extensively used in IaaS cloud in order to integrate/decompose physical resources in an ad-hoc manner to meet growing or shrinking resource demand from cloud consumers. E.g.-Amazon's EC2. Thespecial type of Iaas is **Data storage as a Service (DaaS)** which allows consumers to pay for what they are actually using rather than the site license for the entire database. E.g.-Amazon S3, Google Big Table.

IV. DEPLOYMENT MODEL

The four cloud deployment models have been defined in the Cloud communityi.e:

4.1. Private cloud

The cloud infrastructure is operated solely within a single organization, and managed by the organization or a third party regardless whether it is located premise or off premise. The motivation to setup a private cloud within an organization is to maximize and optimize the utilization of existing in-house resources, security concerns and data transfer cost.

4.2. Community cloud

Several organizations jointly construct and share the same cloud infrastructure as well as policies, requirements, values, and concerns. The cloud community forms into a degree of economic scalability and democratic equilibrium. The cloud infrastructure could be hosted by a third-party vendor or within one of the organizations in the community.

4.3. Public cloud

This is the dominant form of current Cloud computing deployment model. The public cloud is used by the general public cloud consumers and the cloud service provider has the full ownership of the public cloud with its own policy, value, and profit, costing, and charging model

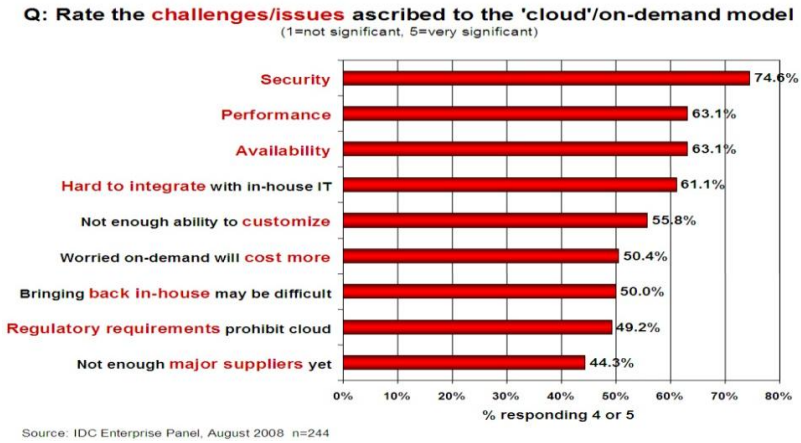
4.4. Hybrid cloud

The cloud infrastructure is a combination of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load-balancing between clouds). Organizations use the hybrid cloud model buthybrid cloud has raised the issues of standardization and cloud interoperability.

Amazon Web Services (AWS) has recently rolled out a new type of deployment model - **Virtual Private Cloud (VPC)**, a secure and seamless bridge between an organization's existing IT infrastructure and the Amazon public cloud. This is positioned as a mixture between Private Cloud and Public Cloud. It is Public because it still uses computing resources pooled by Amazon for the general public. However, it is virtually private for two reasons. Firstly, the connection between IT legacy and the cloud is secured through a virtual private network, thereby having the security advantage of Private Cloud.

V. CLOUD COMPUTING ISSUES & CHALLENGES

Cloud computing is steadily gaining acceptance within businesses. It is predicted that by 2018, 59% of the cloud workloads will be generated from Software as a Service (SaaS). Cloud Computing has already started to revolutionize the way we store and access data. We currently see smartphone applications use cloud computing technology to allow users to store and access data they previously couldn't on a smart device.But cloud computing too comes with its share of issues despite being core strength of some business industries. Issues and challenges of cloud computing are characterized as ghosts in the cloud.



1. **Data security and recovery**

It is clear that security has played the most important role in cloud computing acceptance. The security threats can be of two types like internal and external. The external risk is posed by various persons. For e.g.: hackers that do not have direct access to the cloud. The internal security risk is posed by employees and other parties that have received access to an organization's servers. The cloud provider should be able to answer various questions such as

- Where does your data reside?
- Is the data encrypted?
- How do you move data from the cloud?

So that you know exactly where your data is stored and how they will protect your data against internal and external threats. All the cloud computing service providers must set up their servers at economically stable locations where they should have proper arrangements for the backup of all the data in at least two different locations. Ideally they should manage a hot backup and a cold backup site.

2. Performance

In cloud computing performance is generally measured by capabilities of applications running on the cloud system. Poor performance can be caused by lack of proper resources for e.g.: limited bandwidth, lower C.P.U speed etc. Many times users prefer to use services from more than one cloud where some applications are located on private cloud while other on public.

3. Availability

One way to achieve reliability is redundant resource utilization. Availability can be understood as the possibility of obtaining the resources whenever they are needed with the consideration.

4. Resolving the stress

Every organization wants to have a proper control and access over the data. It is not easy to hand over data to third party. Every enterprise and executives desire to control over the new modes of technology.

5. Access to data

Cloud-based servers do not always have the most effective or appropriate customer service support systems. Selecting where and how your data is stored is an important element within the decision making process.

Integration is a problem for many organizations. Important questions you should ask A cloud provider must know

- How much control do they have over data and server?
- How much time does it take to back up my data to the cloud?
- How long does it take to back up my data?
- Where does my data reside?
- How does the service provider secure my data?

6. Cost barrier

For efficient working of cloud computing you have to bear the high charges of the bandwidth. For smaller application cost is not a big issue but for large and complex applications it is a major concern. For transferring complex and intensive data over the network it is very necessary that you have sufficient bandwidth. This is a major obstacle in front of small organizations, which restrict them for implementing cloud technology in their business.

7. Lack of knowledge and expertise

Every organization does not have sufficient knowledge about the implementation of the cloud solutions. They have not expertise staff and tools for the proper use of cloud technology. Delivering the information and selection the right cloud is quite difficult without right direction.

8.Cloud management

Managing a cloud is not an easy task. Cloud management is the management of cloud computing products and services. Public clouds are managed by public clouds service. Where private clouds are managed by private clouds service

9. Service Quality

Service quality is often one of the most significant factors that businesses cite as a reason for not moving their business applications to the cloud. Often businesses feel as though the SLAs provided by the cloud providers today are not adequate to assure the requirements for running a production application on the cloud, especially those related to availability, performance and scalability.

10.Selecting the perfect cloud set-up

Choosing the appropriate cloud mechanism as per the needs of your business is very necessary. There are three types of clouds configuration such as public, private, and hybrid. The main secret behind successful implementation of the cloud is picking up the right cloud. If you are not selecting the right cloud then maybe you have to face some serious hazards.

11.**Real time monitoring requirements**

In some agencies, it is required to monitor their system in real time. It is compulsory term for their business that they continuously monitor and maintain their inventory system. Banks and some government agencies need to update their system in real time but cloud service providers are unable to match this requirement. This is really a big challenge for cloud services providers.

12.Dependency on service providers

An authorized vendor who can meet the security standards set by your company's internal policies and government agencies. While selecting the service provider you must carefully read the service level agreement and understand their policies and terms and provision of compensation in case of any outage or lock in clauses.

13.Cultural obstacles

High authority of the company and organizational culture has also become a big obstacle in the proper implementation of the cloud computing. Top authority never wants to store the important data of the company somewhere else where they are not able to control and access the data. They have misconceptions in their minds that cloud computing puts the organization at the risk by seeping out important details. Their mindset is such that the organization on risk averse footing, which makes it more reluctant to migrate to a cloud solution.

14. Consumption basis services charges

Cloud computing services are on-demand services. It is not easy for a normal business owner to study consistent demand and fluctuations with the seasons and various events. So it is hard to budget for a service that could consume several months of budget in a few days of heavy use.

15. Hacking of brand

Cloud computing carries some major risk factors like hacking. Some professional hackers are able to hack the application by breaking the efficient firewalls and steal the sensitive information of the organizations. A cloud provider hosts numerous clients; each can be affected by actions taken against any one of them. When any threat came into the main server it affects all the other clients also.

16.Data portability

Ensuring data portability is very necessary. Usually, clients complain about being locked in the cloud technology from where they cannot switch without restraints. There should be no lock in period for switching the cloud. Cloud technology must have capability to integrate efficiently with the on premises. The clients must have a proper contract of data portability with the provider and must have an updated copy of the data to be able to switch service providers, should there be any urgent requirement.

17.Dealing with lock-ins

Cloud providers have an important additional incentives to attempt to exploit lock-ins. A prefixed switching cost is always there for any company receiving external services. Exit strategies and lock-in risks are primary concerns for companies looking to exploit cloud computing.

18.Transparency of service provider

There is no transparency in the service provider's infrastructure and service area. You are not able to see the exact location where your data is stored or being processed. It is a big challenge for an organization to transfer their business information to such an unknown vendor.

19.Transforming the data into virtual set-up

Transition of business data from a premise set up to a virtual set up is a major issue for various organizations. Data migration and network configuration are the serious problems behind avoiding the cloud computing technology.

20. Interoperability and Portability

Businesses should have the leverage of migrating in and out of the cloud and switching providers whenever they want, and there should be no lock-in period. Cloud computing services should have the capability to integrate smoothly with the on premise IT.

VI. CONCLUSION

Cloud computing can be considered as an integral component of almost all businesses which is set to revolutionize the way we use the Internet. It is based on the model of delivering services on internet with pay-as-you go model with advantages like no up-front cost, lower IT staff, lower cost of operation to name a few. There are many new technologies emerging at a rapid rate, each with technological advancements and with the potential of making human's lives easier. However, one must be very careful to understand the security risks and challenges posed in utilizing these technologies. In this paper key security considerations and challenges which are currently faced in the Cloud computing are highlighted. Cloud computing has the potential to become a frontrunner in promoting a secure, virtual and economically viable IT solution in the future.