BEST: International Journal of Management, Information Technology and Engineering (BEST: IJMITE)
ISSN (P): 2348-0513, ISSN (E): 2454-471X,
Vol. 4, Issue 3, Mar 2016, 89-98

AN ANALYSIS OF DEPLOYMENT MODELS IN CLOUD COMPUTING

J. KASHIFA KHURSHID[1] & P. THENMOZHI[2]

[1]M.Phil (Research Scholar), Department of Computer Science, Kongu Arts and Science College, Erode, Tamil Nadu, India

[2]Assistant Professor, Department of Computer Science (UG), Kongu Arts and Science College, Erode, Tamil Nadu, India

ABSTRACT

Cloud computing is a well emerging technology and its main objective is to provide secure, quick, convenient data storage and net computing service. These days cloud computing is booming like no other technology. Each and every organization whether it's small, mid-sized or big, wants to adapt this technology for their business. Now a days more IT companies are upgrading to cloud based service like Private, Public and Hybrid cloud computing as it reduces cost and maintenance of IT industry but at the same time they are facing more security problems. In this paper much attention is given to Public, Private, Community and Hybrid cloud computing issues and given a clear idea about which model is suitable for their organization.

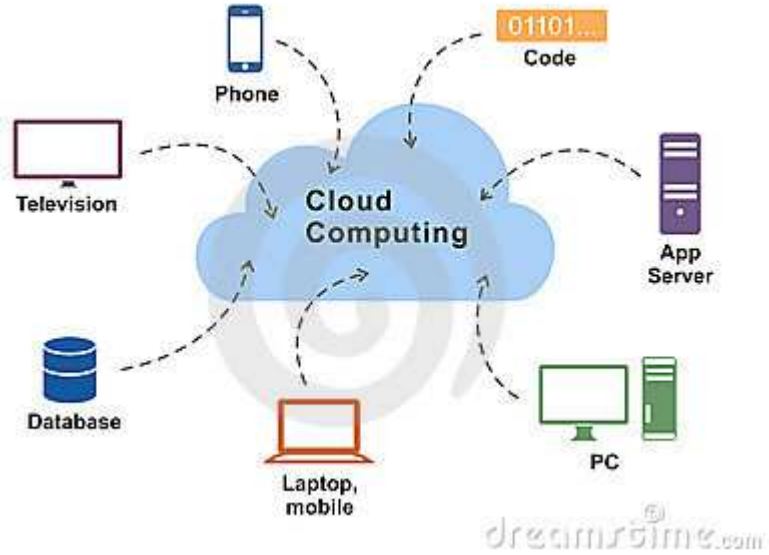
KEYWORDS: Cloud Computing, Security, Public Cloud, Private Cloud, Hybrid Cloud

INTRODUCTION

Now days the term "Cloud Computing" plays an important role in information technology industry. It is widely used by the internet user's community with many different meanings given by different authors. The Cloud Computing reshapes IT industry and in software development process. The aspects of personal life and work are moving towards the concept of availability of everything on the internet. Using this trend the very big web based companies like Google and Amazon came with a model namely "Cloud Computing" the sharing of web infrastructure to deal with the internet data storage, scalability and computation. In Cloud Computing, based on customers demand hardware and software services are delivered through online. Cloud computing effectively reduces the cost and maintenance.

Gartner defines Cloud Computing as being scalable, delivering IT- enabled services using the Internet [1]. On the other hand, Cloud Computing is a set of business models and technologies that enables IT functions to be delivered and consumed via third party [2]. The mostly used definition today is the one expressed by the National Institute of Standards and Technology (NIST), which states: "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, application and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" [3].

Cloud Computing is a distributed computing that mainly focuses on providing a wide range of users to access scalable, virtualized hardware and/or software infrastructure through the internet [4]. By enabling elastic on-demand provisioning of computing resources, Cloud Computing has created huge change in the Information Technology industry [5]. In future we won't compute local computers because of Cloud Computing but only to operate centralized facilities by third-party computation and storage utilities [6].

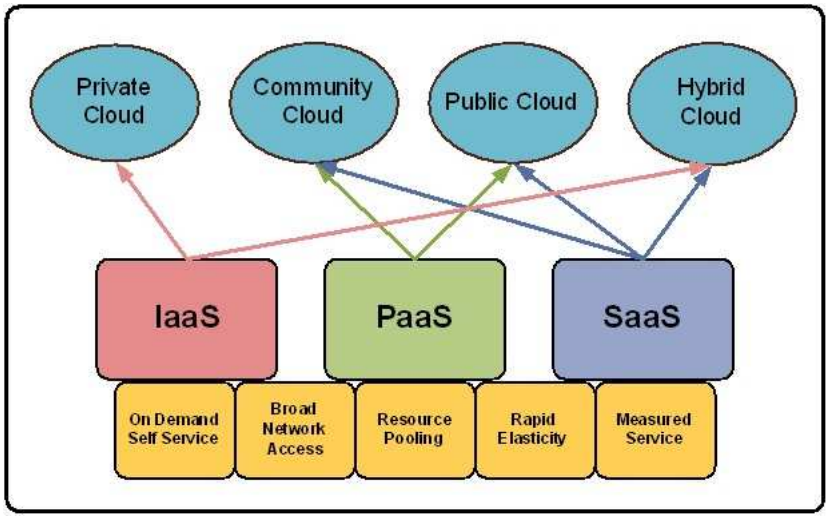


In a cloud computing environment many entities are involved. The cloud consumer is the entity that consumes the resources and may be an individual or an organization. The three basic delivery models for cloud computing are given below.

Infrastructure-as-a-Service (IaaS): It provides the infrastructure (computing platform), resources and tools (servers, storage, network, etc) to build an application environment. Amazon's EC2 is an example of an IaaS

Platform-as-a-Service (PaaS): It provides the computing platform as well as solution stack for consumers to develop their own applications and host their own data. Google Apps is one of the major PaaS providers.

Software-as-a-Service (SaaS): It provides the computing platform and applications to customers for use. Some examples are Facebook, Twitter, and various web-based email systems such as those offered by Google.



CLOUD COMPUTING DEPLOYMENT MODELS

There are four deployment models of cloud computing depending on infrastructure ownership. Each model has its own advantages and disadvantages. This is where the security issues starts.

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 [7]. In public clouds, resources are offered as a service, usually over an internet connection, for a pay-per-usage fee. Users can scale their own on demand and do not need to purchase hardware to use the service. Public cloud providers manage the infrastructure and pool resources into the capacity required by its users [8]. A Public cloud is hosted on the internet and designed to be used by any user with an internet connection to provider a similar range of capabilities and services [9]. Data created and submitted by consumers are usually stored on the servers of the third party vendor [10].

The advantages of Public Cloud include:

- Data availability and continuous uptime
- 24/7 technical expertise
- On demand scalability
- Easy and inexpensive setup
- No wasted resources

Drawbacks of Public Cloud:

- Data security
- Privacy
- Reliability

Another issue with Public cloud is that you may not know where your data is stored or how it s backed up, and whether unauthorized users can get access to it. A recent two-day Amazon cloud outage, for example, left dozens of major e-commerce websites disabled or completely unavailable [11].

Examples of Public Cloud include:

- Amazon AWS
- Google Apps
- Salesforce.com
- Microsoft BPOS
- Microsoft Office 365

Private Cloud

A Private cloud is also called as an “internal cloud” or “corporate cloud”, resides within the company environment. The private cloud is a cloud infrastructure operated solely for a single organization, whether managed internally or by a third-party and hosted either internally or externally [7]. The cloud infrastructure is accessed only by the members of the organization and/or by granted third parties. The purpose is not to offer cloud services to the general

public, but to use it within the organization. A Private cloud is hosted in the data center of a company and providers its services only to users inside that company or its partners. A private cloud providers more security than public clouds, and cost saving is based on utilization of data center. Over the last several years, major cloud services breaches have dominated the headlines. Corporations are taking notice and some are deciding that the private cloud proves less risky. Private cloud's ability to virtualized services maximizes hardware usage, ultimately reducing costs and complexity.

The advantages or Private Cloud:

- Improved security and privacy
- Greater control over the server
- Flexibility in the form of Cloud Bursting
- Cost and energy efficiency
- Improved reliability

Disadvantages of Private Cloud:

- Higher cost

When comparisons are made with Public cloud; the cost of purchasing equipment, software and staffing often results in higher costs to an organization having their own Private cloud.

Examples of Private Cloud include:

- Amazon Virtual Private Cloud (Amazon VPC)
- Cisco Private Cloud Solutions
- Dell Cloud Solutions
- IBM SmartCloud Foundation
- Red Hat Cloud

Hybrid Cloud

Hybrid clouds are more complex than the other deployment models, since it is a combination of two or more clouds (private, community or public). Each member contains a unique entity, and at the same time they are bound together by standardized technology that enables application and data portability among them [13]. For example, organizations that have their human resource (HR) and customer relationship management (CRM) data in a public cloud like Salesforce.com but have confidential data in their own private cloud. Hybrid cloud [14] offer the cost and scale benefits of public clouds, while also offering the security and control of private clouds.

The advantages of Hybrid Cloud:

- More scalable in terms that it contains both Private and Public clod.
- Offers both secure resources and scalable Public resources.

- Provides always a highest level of security as it has designated Private cloud.
- Reduce and manage the cost based on the requirement.

Disadvantages of Hybrid Cloud:

- Infrastructure dependency
- Security compliance
- Networking

Hybrid clouds offer a greater flexibility to businesses while offering choice in terms of keeping control and security.

Examples of Hybrid Cloud:

- Google Compute Engine
- Amazon S3
- IBM and VMware
- Apple Swift

Community Cloud

A community cloud falls between public and private clouds with respect to the target set of consumers. It is somewhat similar to a private cloud, but the infrastructure and computational resources are exclusive to two or more organizations that have common privacy, security, and regulatory considerations, rather than a single organization [15]. The community cloud aspires to combine distributed resource provision from grid computing, distributed control from digital ecosystems and sustainability from green computing, with the use cases of cloud computing, while making greater use of self-management advances from autonomic computing. Replacing vendor clouds by shaping the under utilized resources of user machines to form a community cloud, with nodes potentially fulfilling all roles, consumer, producer, and most importantly coordinator [16].

The advantages of Community Cloud include:

- Cost of setting up a communal cloud versus individual private cloud can be cheaper due to the division of costs among all participants.
- Management of the community cloud can be outsourced to a cloud provider. The advantage here is that the provider would be an impartial third party that is bound by contract and that has no preference to any of the clients involved other than what is contractually mandated.
- Tools residing in the community cloud can be used to leverage the information stored to serve consumers and the supply chain, such as return tracking and just-in-time production and distribution.

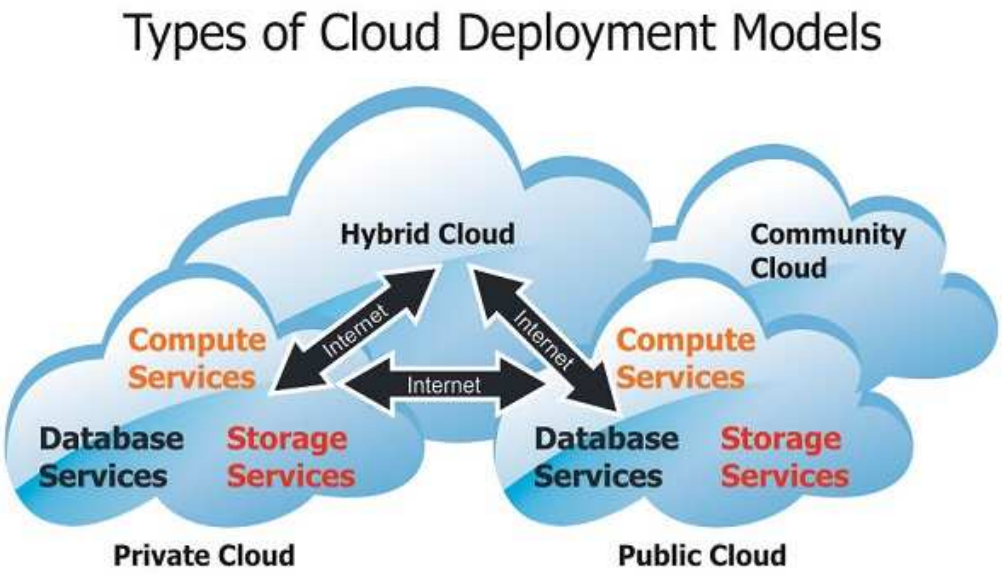
Disadvantages of Community Cloud:

- Costs higher than public cloud.
- Fixed amount of bandwidth and data storage is shared among all community members.

The concept of community cloud is still in its infancy, but picking up rapidly among start-ups and small and medium term businesses.

Examples of Community Cloud:

- Google
- RedHat
- Microsoft
- IBM



SECURITY ISSUES IN DEPLOYMENT MODELS OF CLOUD COMPUTING

Public Cloud

Public Clouds are hardened through continual hacking attempts. Public Cloud providers are much larger targets for hackers than private Clouds. Public clouds also attract the best security people available; the biggest and best Clod service providers have millions of customers relying on them.

Assessment of the Cloud Service Provider

The young and small business can advertise Cloud-based services to the world. Hence cloud service provider (CSP) should hold industry necessary certifications such as the SAS 70 Type II [11], which is an audit that providers independent 3rd party verification that a service organization's policies and procedures are correctly designed.

Security of the Communication Channels

Data and Communication protection plays a vital role in Cloud computing. Services can be accessed through a thin client, laptop or mobile phones. All communication should be protected using encryption and key management.

Compliance with Regulations

Payment card Industry Data Security Standard (PCIDSS). Sarbanes – Oxley Act (SOA). Proper implementation of the CIA triad (Confidentiality, Integrity, Assurance). Geographical borders – the location of the customer's data is significant.

Data Loss

Weakness of shared network infrastructure components, such as weakness in a DNS server, Dynamic Host Configuration Protocol and IP protocol weaknesses, may be enabled network-based cross-tenant attacks in an IaaS infrastructure.

Private Cloud

Private Clouds have the same security concerns as public Clouds. However, there are some specific security issues towards this Private Cloud model. As per the social TechNet articles the areas where IT decision makers have bear in mind with implementation of private cloud, are legality, data protection and compliance. The following are some thoughts on making some security changes in private cloud. They are i) Beyond the issues of scalability and consistency, patch management, configuration management should also be considered. ii) The integrity and security of hypervisor need also be considered. iii) In cloud management platform, the amount of automation is also to be secured. iv) Stringent control should be in place of Hypervisors to ensure security.

Security Control

The organizations those who are using private cloud infrastructure should need to ensure that effective control of the new environment. The private cloud management architecture should enable management to view security aspects of the environment and show the current threat levels to the organization. The control oversight is to be provided through a web based dashboard that translates the security issues into understandable languages.

Compliance

Organizations such as health and financial operations fall under the auspices range of agreement requirements and regulations. With international organization it is possible that moving to private cloud different set of regulations may be followed by different countries to access data.

Hybrid Cloud

Trend Micro, a cloud security company, recently conducted a survey which indicated that public cloud services fail to meet IT and business requirements of some of the business organizations. A hybrid cloud environment can help meet their needs.

Absence of Data Redundancy

Problems are inevitable for any cloud providers even though they took best efforts. Hybrid cloud is a complex system. That management has limited experience in managing and that creates great risk. Cloud architects need redundancy across data centers to moderate the impact of an outage in a single data center. A lack of redundancy can become a serious security risk in hybrid cloud, specifically if redundant copies of data are not distributed across data centers. It's easier to move virtual machine (VM) instances between data centers than between large data sets.

Compliance

In a hybrid cloud maintaining and demonstrating compliance are more difficult. Not only you have to ensure that your public cloud provider and private cloud are in compliance, but you also must demonstrate that the means of coordination between the two clouds is compliant.

Risk Management

Information security is very difficult to manage risk for a business perspective. Cloud computing (hybrid cloud in particular) uses new application programming interfaces

(APIs), requires complex network configurations, and pushes the limits of traditional system administrators' knowledge and abilities. These factors introduce new types of threats.

COMMUNITY CLOUD

Community Clouds can be used by either a single-tenant (dedicated) or multi-tenant (shared) operating environment which are provided by service provider with all the benefits and functionality of elasticity and the accountability/utility model of cloud. The physical infrastructure is owned by and/or physically located in the organizations' data centers with an extension of management and security control planes controlled by the designated service provider. When assessing the impact a particular cloud service may have on one's security posture and overall security architecture, it is necessary to classify the assets/resource/service within the context of not only its location but also its criticality and business impact as it relates to management and security. This means that an appropriate level of risk assessment is performed prior to entrusting it to the vagaries of the cloud (CSA Security Guidance, 2009). In addition, it is important to understand various tradeoffs between the various cloud service models:

- Generally, SaaS provides a large amount of integrated features built directly into the offering with the least amount of extensibility and in general a high level of security (or at least a responsibility for security on the part of the service provider).
- PaaS offers less integrated features since it is designed to enable developers to build their own applications on top of the platform, and it is, therefore, more extensible than SaaS by nature. However, this extensibility features trade-offs on security features and capabilities.
- IaaS provides few, if any, application-like features, and provides for enormous extensibility but generally less security capabilities and functionalities beyond protecting the infrastructure itself, since it expects operating systems, applications and contents to be managed and secured by the customers.

COMPARISON OF PUBLIC, PRIVATE, HYBRID AND COMMUNITY CLOUDS:

- Security – To make sure the legal data jurisdiction issues are addressed by the hosting site.
- Elasticity – To allow application writers to move easily through test/dev. to production and allow for Web scale growth.
- Performance –To run applications synchronously or asynchronously at appropriate speeds.

CONCLUSIONS

Organizations willing to adapt cloud model for their enterprise often feel confused, which model will fit best for their business. To help business organizations take this decision, this review was planned. Now a days Cloud Computing technology is adapted in every organization for their business profitability and scalability. This communication defined cloud computing, highlighted all the service models of cloud computing and discussed the features of public, private, hybrid and community cloud computing. Also, cloud security issues were raised and discussed. Technology-wise, there is not much significant difference among these four models. They all run on the same technology, one of the pitfalls of adopting a public cloud is data security and privacy. On the other hand private cloud is secure, but costly, so not every organization can afford a private cloud. Hybrid cloud is a mixture of public and private cloud; organizations keep their regular data in the public cloud and use private cloud to keep their sensitive data in hybrid model. Similarly a community cloud falls between public and private cloud, as some organizations get together and form a separate private cloud of their own, called a community cloud.

REFERENCES

1. Gartner (2012) Cloud Computing. Retrived April 15, 2012 from http://www.gartner.com/technology/it-glossary/cloud omputing.jsp.
2. Rhoton, J. (2011). Common definition. Cloud Computing Explained: Second edition. Recursive Press, Us.
3. Grance, T., Mell, P.(2009) The NIST Definition of cloud computing. Retrieved march15, 2012 from http://www.nist.gov/itl/cloud/upload/cloud-def-v15.pdf.
4. Ernst and Young (2011). In to the cloud, out of the fog. Retrieved April 13, 2012 from http://www.ey.com/GL/en/Services/Advisory/2011-Global-Information-Security-Survey-seeing-through-the-cloud.
5. Journal of Emerging Trends in Computing and Information Sciences, VOL. 2, NO. 10, October 2011pp 546-552and Search cloud computing.com E- Guide.
6. SAS 70 (2012). *Introduction to SAS 70 Type II Audit.* Retrieved April 16, 2012 from http://www.sas70exam.com/ services/type-ii- sas-70-audit/.
7. P. Mell and T. Grance, ―"The NIST definition of cloud computing (draft)", NIST special publication, 800(145), 7, 2011.
8. G. Lewis, ― "Basics about cloud computing", Software Engineering Institute Carniege Mellon University, Pittsburgh, 2010.
9. (2013) Open Cloud Manifesto. [Online]. Available: http://www.opencloudmanifesto.org/.
10. O. Hamrén. (2012). M.S. Thesis. ―"Mobile phones and cloud computing".
11. (2013) Aberdeen Website. [Online]. Available: http://www.aberdeen.com/Research/Research-Library.aspx?search=private%20cloud.
12. W. Jansen and T. Grance, ―"Guidelines on security and privacy in public cloud computing", NIST special

publication 800-144, 2011.

13. (2013) Emma TrendMicro Website. [Online]. Available: http://emea. TrendMicro. com/imperia/md/content/uk/cloud security/wp01_hybridcloud-krish_110624us. Pdf
14. W. Jansen and T. Grance, ―Guidelines on security and privacy in public cloud computing,‖ NIST special publication 800-144, 2011.
15. A. Marinos and G. Briscoe, ―Community cloud computing,‖ In: Cloud Computing (pp. 472-484). Springer Berlin Heidelberg, 2009.