Security Issues: Public vs Private vs Hybrid Cloud Computing

R.Balasubramanian
ME in Computer Science
M S University,Tamilnadu,India.

M.Aramudhan, PhD.
ME in Computer Networks
P K I of Engg& Tech. Karaikal, Pondicherry, India

ABSTRACT

Cloud computing appears as a new paradigm and its main objective is to provide secure, quick, convenient data storage and net computing service. Even though cloud computing effectively reduces the cost and maintenance of IT industry security issues plays a very important role. More and more IT companies are shifting to cloud based service like Private, Public and Hybrid cloud computing. But at the same time they are concerned about security issues. In this paper much attention is given to Public, Private and Hybrid cloud computing issues., as more business today utilize cloud services and architectures more threats and concerns arise. An analysis of comparative benefits of different styles of cloud computing by using SPSS is also discussed here.

General Terms

Computer Networks

Keywords

Cloud computing, Security, SPSS, TCO

1. 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 aspectsof personal life and work are moving towards the concept of availability of everything on the internet. Using this trend the verybig web based companies like Google andAmazon came with a model namely "Cloud Computing" the sharing of web infrastructure to deal with the internet data storage, scalability and computation. Cloud Computing is an online service model by which hardware and software services are delivered to customers depending upon their requirements.Cloud computing effectively reduces the cost and maintenance.

Many definitions of Cloud Computingfocus on certain characteristics of it. We can see that some definitions have more meaning than others. Gartner defines Cloud Computing as being scalable, delivering IT- enabled services using the Internet (Gartner [1], 2012). 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(Rhoton,J.[2] 2011). 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" (Grance,T., Mell.P.,[3],2009)

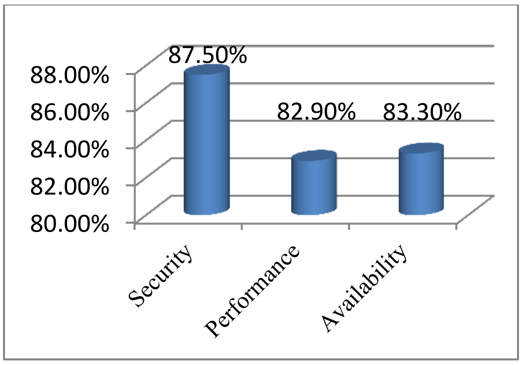
In a cloud computing environment many entities are involved. We are very much interested particularly in the cloud provider and the cloud consumer. The cloud provider is the entity which owns and manages the resources. The cloud consumer is the entity that consumes the resources and may be an individual or an organization. When a cloud consumer is an organization, it will have users or employees that access cloud resources. There may be casual users that have no relationship with the cloud provider, but are accessing cloud consumers' web services that are developed and hosted within the cloud. Here the security and trust relationship of concern is between the cloud provider and the cloud consumer.

Several research papers and magazine articles are available to discuss cloud computing in detail. The three basic delivery models for cloud computing are given below.
Infrastructure-as-a-Service(IaaS): It providesthe 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 platformandapplicationstocustomers
for use. Some examples are Facebook, Twitter, and various web-based email systems such as those offered by Google.

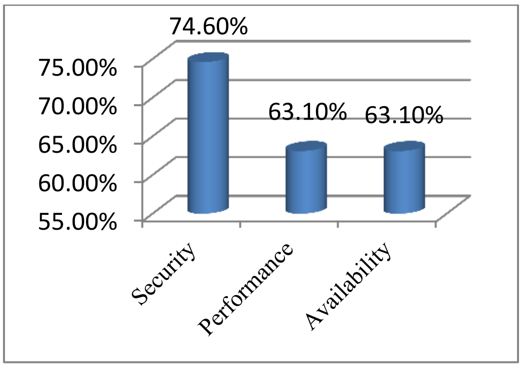
2. SECURITY ISSUES IN CLOUD COMPUTING

The main factor for IT Executives when it moves to cloud computing is security and privacy. It environments are multi domain environment in which various resources are shared. While sharing Hardware and placing data it seems to be a highly risk factor. Any unauthorized person can easily hacked either accidently or due to malevolent attack. Hence data storage would be a major security violation. By considering this security issues, two surveys were carried out by IDC in 2008 and 2009. Their observations are analyzed and presented here.



Source: IDC Enterprise Portal, 2009

Fig.1 Rate of challenges/issues with the cloud/on-demand model in 2009



Source: IDC Enterprise Portal, 2008

Fig.2 Rate of challenges/issues with the cloud/on-demand model in 2008

IDC conducted a survey of 244 IT executives/CIOs and their line of business colleagues about their companies' use of and views about IT cloud services. They have asked to rate the challenges/issues endorsed to the cloud/on-demand model. By comparing these two surveys, we observe from the above figures (see fig. 1 and 2) thatsecurity challenges seem to be the top. The rate of all the three challenges was increased where as in 2008 Performance and Availability were tied. From their survey we understand that the cloud providers should take much more care for security of data stored in cloud.

When considering vendor's services for cloud computing, the consulting firm and technology analyst should bear the following security issues in their mind.

They have to enquire about who has access to data and about hiring and management of such administrators.
You have to ascertain whether thevendor is willing to undergo external audits and / or security certification.

Ask your cloud provider allows for any control over the location of data.
You have to confirm that encryption is available at all stages and that these "encryption schemes were designed and tested by experienced professionals'

Check out what will happen to data in the case of disaster. Do they offer complete restoration and if so, how long that would take.

Ask whether a vendor has the ability to investigate any inappropriate or illegal activity.

Examine what will happen to data if the company goes out of business. How will data be returned and in what format?

3. MAIN TYPES OFCLOUD COMPUTING

The three main types of cloud computing has been studied and point out in the following sub sections. This subsection gives us
a clear idea about different types of cloud computing.

3.1 Public Clouds

One of the standard cloud computing models is a Public cloud. Here the service provider makes resources like application, infrastructure and storage, available to the customers and businesses over the internet. The service providers like Microsoft, Google etc. have their own infrastructure at their data center. The access will be only through internet mode. There will be no direct connectivity is proposed in Public cloud architecture.The services may be offered free (Gmail) or may be provided as pay per use facilities to businesses. Here, the customer has limited visibility into or control over where the computing infrastructure is hosted. Although public cloud services are easy to administer and cost effective, they are not considered as secure as private clouds.

3.2 PrivateClouds

It is a cloud computing platform built on your own hardware and software. It is also known as internal cloud or corporate cloud. It provides hosted services to a limited number of people behind a firewall. When you require greater level of security and control over your applications, this type of cloud is most preferable. Here, the services and infrastructure provided are maintained over a private network and are generally used by corporate houses. This private cloud services is more costly because we need to buy, build and manage them. However, the reliability offered makes them popular and given them potential as a growing market.

3.3 Hybrid Clouds

When you wish to maintain different business applications with different levels of securityparticularly this service is useful. Hybrid clouds services are a combination of public and private clouds implemented by different providers. One of the disadvantages of these services is that we have to manage different security platforms together.

4.GROWTH OF CLOUD COMPUTING

Ernst and Young's 2011[4] global information security survey was conducted between June 2011 and August 2011. As per their survey nearly 1700 major organizations and 52 countries were participated. The region wise participants are 29% Americans, 20% Asia pacific, 44% EMIEA and 7% Japan. As per its survey the organizations currently use cloud computing services in terms of percentage for 2010 and 2011 are presented in the followingfigure.

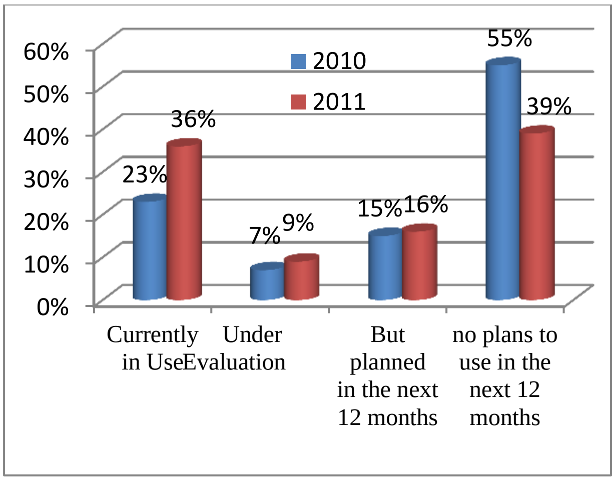


Fig.3 Organization currently use cloud computing – based survey. Comparison between 1010 and 2011

From the above Fig. 3 we observe that there is a 13% positive growth in the number of organizations using cloud based service from 2010 to 2011. But there was a 16% negative growth for no plans on using cloud based services. From this we can predict the positive growth in the forthcoming year 2012 provided if the growth is linear trend.

5. 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.

5.1 Public Cloud

Most of the IT department executives are concerned about the public cloud security and reliability.It is usually owned by a very big organization such as Amazon's EC2, Google's and AppEngine etc. The owner of the organization makes the public cloud infrastructure available to the customers over the internet via self-service basis multitenant model. This is the most cost effective model leading to security issues. It is suitable choice when to test and develop application code, SaaS applications from a vendor who has implemented securitystrategy, doing collaboration project and doing an ad-hoc software development project.

5.2Private Cloud

The services and infrastructure are maintained on a private network in a Private cloud. It offers the greatest level of security and control. But here the company has to purchase and maintain all software and infrastructure which reduces the cost savings. It is a single tenant environment. It maybe managed by the tenant organization or by a third party within or outside the tenant premises. A private cloud incurred more cost than the public cloud. But it leads to more cost savings when compared with a datacenter. It is suitable when business is your data and application so that control and security are supreme.

5.3 Hybrid Cloud

It is a combination of the above discussed two cloud computing environments where some data resides in the private cloud environment and some resides in the public cloud environment. It is usually a combination of on-and off-premise. A comparison of the different issues of cloud computing on cloud deployment models is given below.

Table 1 .Cloud Deployment models and issues

Model	Security issues	Cost issues	Control issues	Legal issues
Public	i)Least secure ii)Multi-tenancy iii)Transfers over the net	Setup:Highest Usage: lowest (pay for what you use)	Least control	Jurisdiction of storage
Private	Most secure	i)Setup: High ii)New operational processes are required	Most control	--
Hybrid	Control of security between Private and Public clouds	--	Least control	Jurisdiction of storage

Source: Journal of Emerging Trends in Computing and Information Sciences, VOL. 2, NO. 10, October 2011pp 546-552and Search cloud computing.com E- Guide[5]

From the above table it is understood that private cloud has more secure than public. According to the cost issues the setup cost is very high in both private and public. If we consider control issues private cloud is most control than public and hybrid clouds. But public and hybrid clouds have same legal issues.

6. SECURITY ISSUES: PUBLIC CLOUD

Usually there is an ongoing debate between IT professionals of whether or not private Clouds are really more secure. Besides from the common view that private Clouds should be more secure, there are some interesting attributes/properties of public Clouds to consider.

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 Cloud service providers have millions of customers relying on them. They definitely would be meticulous about who they hire. Also public Cloud providers, especially larger companies like Google, Amazon, and Facebook would get the latest security gear much easier than a small to midsize private company. Here are some other security issues related to Public Cloud Computing:

6.1 Assessment of the cloud service provider

The young and smallbusiness can advertise Cloud-based services to the world. But how can you asses thatthe company is capable and safe to work with? Hence cloud service providers (CSP) should hold industry necessary certifications such as the SAS 70 Type II[6], which is an audit that provides independent 3rd party verification that a service organization's policies and procedures are correctly designed.

6.2 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 phone. The reasons that your data is easily accessible through these channels are your data is transferred across multiple networks, more especially if your CSP is extremely far away from your location. All communication should be protected using encryption and key management.

6.3 Transparency of security processes

Some Cloud Service Providers may not be able to explain their security processes for their own security reasons.

6.4 Compliance with Regulations

- ✓ Payment Card Industry Data Security Standard (PCI DSS)
- ✓ Health Insurance Portability and Accountability Act (HIPAA)
- ✓ Sarbanes-Oxley Act (SOA)
- ✓ Proper implementation of the CIA triad (Confidentiality, Integrity, Assurance)
- ✓ Geographical borders - The location of the customer's data is significant. To safe guard server failure Public Cloud service providers will typically implement strong data replication mechanisms. This means that the customer's data might be distributed across the globe in various geographies. This would conflict with the customer's need/requirements to keep their data within a specified border(Microsoft Corporation,2011[7].

6.5 Potentials of a single security failure

During 2011 a new report from Privacy Rights Clearinghouse (PRC) says that companies must place on creating" straight privacy and security polices" as well as data holding polices. Also businesses could avoid "violates" simply by properly encrypting all sensitive information. Also we have to note that if encrypted data gets lost or stolen, it will not count ina data failure. Some examples for security violates are i) Sony data failures in 2011 and faced customer relation fallouts. ii) The cloud based email service provider Epsilon faced a problem of 60 million customer emails addresses were violated. iii) Data from both Sutter physicians Services and Sutter medical foundation was violated which contained about 3.3 million patient's medical details. The security lapse happened in two levels: both the data itself (being unencrypted) and the physical location (stored in an unsecure location)

6.6 Data Loss :Cross-tenant data leakage

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

7. SECURITY ISSUES: 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 data protection company discussed the new security issues of private cloud. 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 isalso to be secured.iv) Stringentcontrol should be in place of Hypervisors to ensure security.

Gabriel consulting group recently made survey regarding the security issues inprivate cloud builders. The survey says that 38% organizations are using private cloud. Regarding the serious doubts about the security of their private cloud, their survey reveals that more than 40% organization says that they need cloud security improvement and also about 8% say that the cloud security is very weak in private cloud. Respondents who are planning to build a private cloud, 40% organizations believe that their internal cloud security is very strong.

7.1 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.

7.2 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.

8. SECURITY ISSUES: 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. In some ways, hybrid clouds can be considered an intermediate stage as enterprises prepare to move most of their workloads to public clouds.

8.1Trend Micro Survey results

The Trend Micro[8]conducted a survey in six different countries with 1200 respondents from companies with at least 500 employees. Some of the key results are:

- 38% of the survey respondents say that their IT requirements are not being met by thecloud providers.
- Similarly, 38% claimed that their current cloud service providers are notmeeting their business needs.

- For companies that have public cloud or hybrid applications currently in production, 45%of the existing applications are already deployed in the cloud and an average of 53% of new applications will be deployed in the cloud.
- 49% of the survey respondents indicated that if they knew how to secure their data in the cloud, it would increase their consideration for cloud adoption. Companies are realizing that the use of a hybrid cloud expands the number of applications they deploy into the cloud. However, almost half (49%) feel they need to improve their knowledge of cloud security to further increase cloud adoption.

8.2 Grazed from TechTarget Results

Dan Sullivan[9]suggested that some IT admins are thinking about turning over all their production applications to a third party or losing their substantial investment in on-premises infrastructure. In such cases, a hybrid environment can capitalize on the benefits of both public and private cloud. But hybrid cloud isn't perfect; it still includes a few security obstacles. Hence if any business maintaining a hybrid cloud, they have to keep the following five security issues in their mind.

8.2.1 Hybrid cloud security issue 1: 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.

Cloud architects can implement redundancy using multiple data centers from a single provider or multiple public cloud providers or a hybrid cloud when you improve business continuity with a hybrid cloud, that shouldn't be the only reason to implement this model. You could save costs and attain similar levels of risk mitigation using multiple data centers from a single cloud provider.

*8.2.2 Hybrid cloud security issue 2: 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.

For example if your company works with payment card data, you may be able to demonstrate that both your internal systems and your cloud provider are compliant with the Payment Card Industry Data Security Standard (PCI DSS). You have to ensure that the data moving between two clouds is protected with the introduction of a hybrid cloud..

In addition to that you'll need to ensure that card data is not transferred from a compliant database on a private cloud to a less secure storage system in a public cloud. Also the methods you use to prevent a leak on an internal system may not directly translate to a public cloud.

8.2.3 Hybrid cloud security issue : poorly constructed SLAs:

You have to be very confident that your public cloud provider can consistently meet expectations detailed in the service-level agreement (SLA. Ascertain your private cloud live up to that same SLA. If not, you may need to create SLAs based on expectations of the lesser of the two clouds and that may be your private cloud.Collect data on your private cloud's availability and performance and look for potential problems with integrating public and private clouds that could disrupt service. For example, if a key business driver for the private cloud is keeping sensitive and confidential data on-premises, then your SLA should reflect the limits to which you can use public cloud for some services.

8.2.4 Hybrid cloud security issue 4: 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.

8.2.5 Hybrid cloud security issue 5: Security management:

The existing security controls such as authentication, authorization and identity management should work in both the private and public cloud. To integrate these security protocols, we have one of two options: Either replicate controls in both clouds and keep security data synchronized, or use an identity management service that provides a single service to systems running in either cloud. Allocate sufficient time during your planning and implementation phases to address what could be fairly complex integration issues.

9. COMPARISON OF PUBLIC, PRIVATE AND HYBRID CLOUDS

Security – **T**o 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

According to IT Candor Acronym Buster a comparative benefits of different styles of cloud computing are presented here (see table 2, fig 4)

9.1 Private Cloud

Chief Officers in large companies are often confused about which type of Cloud Computing to adopt within their organization. The largest systems suppliers, such as IBM, HP, Fujitsu are in the process of helping their largest customers build their own private clouds. They are interested to modify existing IT systems and data centers to give more modern experiences for their employees and customers. The scores of using private cloud are as follows.

9.1.1Security 5.0 –There are many health sector, financial and government organizations for which absolute data security requires things to be done in-house.

9.1.2Elasticity 1.0 – Running your own servers there are some handful of vendors such as Hitachi in the storage systems market for instances who may willing to install equipment at your site which you pay for only when you use it.

9.1.3Performance 4.0– performance can be planned as part of the build out of course, although again it will be limited in comparison with some of the of premise solutions

9.1.4Total Cost of Ownership 1.5(TCO)– The score of this is 1.5 as you'll be investing in new systems and processes; there are few examples of 'spend to save' in this area

9.2 Public Clouds

Early Cloud Computing offerings from Sun, Google and Amazon offered application developers the opportunity to develop applications 'on the Cloud' before deploying them. The interview with Double Take Software demonstrates how a supplier can offer asynchronously replicated servers as an alternative to more expensive in-house fault tolerant solutions. The score on Public Clouds are as follows:

9.2.1Total Cost of Ownership 5.0– applications delivered from Public Clouds are almost always the cheapest and have the additional advantage in the recession of being charged on a usage basis: lower

9.2.2Elasticity 5.0– Amazon and Google have massive resources and it is unlikely that you will run out of their capacity to deliver your applications.

9.2.3Performance 2.0 – currently Public Clouds offer little direct control over resources and there may be long distances between your users and the supplier's servers, as a result we've scored performance lower than Hybrid cloud.

9.2.4 Security 1.5– for many organizations Security is a gating factor; financial services companies are legally required to have their systems audited; in many countries you are not allowed.

9.3 Hybrid Private Clouds

There are many types of hybrid Cloud Computing, where an organization keeps control of some – while outsourcing other resources to provide applications to their users. There are twotypes – one where workloads are shared across the customer's and supplier's data center and the other where the vendor takes over the running of the client's systems in a multi-tenanted environment. The involvement of the supplier adds the Public, while knowing where the data and processing takes place ads to the Private elements. Hybrid Clouds tend to offer better TCO than Private Clouds and can achieve acceptable levels of security for many companies. In particular:

The Hybrid Private Cloud, located on and off premise scored almost as highly as the Private Cloud for Security (4.5 v 5.0), although the Elasticity of the system scored 3.0 and the TCO was just 2.0; Performance was highest in Hybrid Private and Hybrid multi-tenant.

The Hybrid Multi-Tenant Cloud is one where the computing is done exclusively in the supplier's data center, sharing many resources with other customers; it has the second lowest score for Security (3.5), but has scored highly in all other categories.

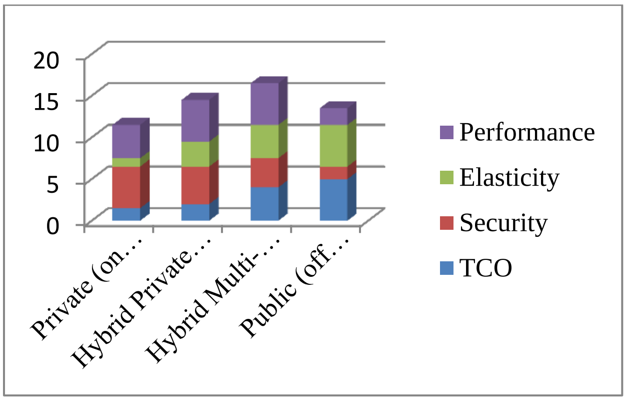


Fig 4. Chart for comparison of scores of different clouds

10. COMPARATIVE ANALYSIS OF DIFFERENT STYLES OF CLOUD COMPUTING

The analysis of data (see table 2)from *IT Candor, November 2010*[10] by using Statistical Packages for Social Sciences(SPSS) of different styles of cloud computing was carried out and various findings are presented here.

Table 2 :The Comparative Benefits of Different Styles Of Cloud Computing

Area	**Private** (on premise)	**Hybrid Private** (on/off premise)	**Hybrid Multi-Tenant** (off premise)	**Public** (off premise)
TCO	1.5	2.0	4.0	5.0
Security	5.0	4.5	3.5	1.5
Elasticity	1.0	3.0	4.0	5.0
Performance	4.0	5.0	5.0	2.0
Average	2.9	3.6	4.1	3.4
Standard Deviation	1.93	1.38	0.63	1.89

Source: ITCandor, November 2010

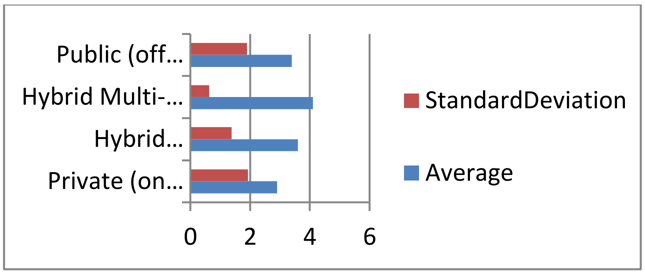


Fig 5. Comparison of Standard Deviation and Averages

From the fig 5 the observations are as follows:

- The highest average scores were the two hybrid models, which offer savings over Private Clouds while retaining adequate levels of security for many.
- The highest average scoring of the four types of Cloud Computing is the Hybrid Multi-Tenant model, where the gating function is the sharing of resources with other users.
- The least standard deviation scoring of the four types of cloud computing is the Hybrid Multi-Tenant model.
- The rank of security of Private, Hybrid Private , Hybrid Multi-Tenant and Public are 1,2,3and4 respectively.

The two ways Analysis Of Variance (ANOVA) was carried out by using Statistical Package for the Social Sciences (SPSS) for table 2 and the results are as follows:

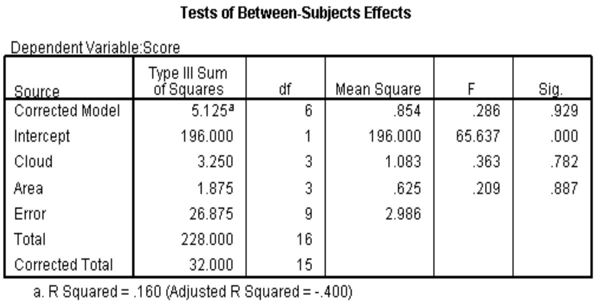
Null Hypothesis (H_o):

a) No significant difference between different types of cloud computing scores.

b) No significant difference between different types of area ie)TCO, Security, Elasticity and Performance.

The output of ANOVA by using SPSS is given in table 3

Table 3. Output of SPSS



Tests of Between-Subjects Effects

Dependent Variable:Score

Source	Type III Sum of Squares	df	Mean Square	F	Sig.
Corrected Model	5.125^a	6	.854	.286	.929
Intercept	196.000	1	196.000	65.637	.000
Cloud	3.250	3	1.083	.363	.782
Area	1.875	3	.625	.209	.887
Error	26.875	9	2.986		
Total	228.000	16			
Corrected Total	32.000	15			

a. R Squared = .160 (Adjusted R Squared = -.400)

Inference:

i) Since the estimated value 0.363 is less than the F table value for d.f (3,9) at 5% level of significance = 3.865 we accept our Ho (a) and we may infer that there is no significant difference between different types of cloud computing scores.

ii) Since the estimated value 0.209 is less than the F table value for d.f (3,9) at 5% level of significance = 3.865 we accept our Ho (b) and we may infer that there is no significant difference between different types of area scores.

11. CONCLUSION

In this paper we have provided a basic definition of cloud computing and discussed the security issues/concerns related to public clouds, private clouds and hybrid clouds. Different kinds of issues related to cloud deployment models are also shown in Table 1. The three cloud models have their own merits and challenges. Therefore security will always be an issue. Various security issues of private, public and hybrid clouds have been discussed. Comparative analysis of three clouds is also given by using SPSS. As far as security concerns private (on premise) cloud has highest score as per IT Condor, November 2010 survey.

Further we present some future ideas that aim to estimate the future trend regarding security issues and growth of cloud computing by using the time series analysis.

12. 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] Microsoft Corporation (2011) *Addressing Cloud Computing Security Considerations*. Retrieved April 2, 2012 from http://search.microsoft.com/en-us/results.aspx?form=MSHOME&setlang=en-us&q=Addressing%20Cloud%20Computing%20Security%20Considerations

[8] www.trendmicro.com/cloud content/us/pdfs/business/white-papers/wp-hybrid -cloud-analysts-subramanian.pdf

[9] www.security.com/content/hybrid-cloud-its-not-secure-you-think

[10] http://it candor.net/2010/11/22 cloud-computing benefits-q410/