Cost breakdown of Public Cloud Computing and Private Cloud Computing and Security Issues

Swarnpreet Singh[1]and Tarun Jangwal[2]

[1]Assistant Professor, CT Institute of Engineering and Management Technology, Jalandhar.
er.swarnsaini@gmail.com

[2]Assistant Professor, CT Institute of Engineering and Management Technology, Jalandhar.
tjangwal@gmail.com

Abstract

The focus of this paper is to distinguish between the issues of private and public cloud computing and what are the challenges faced during Building up your own private and public cloud. which computing out if above two should be implemented in an organization.[12]

Keywords

Public vs. Private cloud computing, Issues in private and public Cloud computing

1. Introduction

1.1 Defining Cloud Computing

Cloud computing refers to both the applications delivered as services over the Internet and the hardware and systems software in the data centers that provide those services. These services have long been referred to as Software as a Service (SaaS). Some terms such as PaaS (Platform as a Service) and IaaS (Infrastructure as a Service) are used by vendors to describe their products, but we avoid these because accepted definitions for them still vary widely. There is no crisp line between "low-level "infrastructure and a higher-level "platform ". We believe both of these are more alike than different, and we do consider them together. Similarly, some related term such as "grid computing," from the high-performance computing community, suggests protocols to offer storage over long distances and shared computation, however those protocols did not lead to a software environment that grew beyond its own community. The data center hardware and software is what we will call a *cloud*. When a cloud is made available in a pay-asyou- go manner to the general public, we call it a *public cloud*; the service being sold is *utility computing*. We use the term *private cloud* to refer to internal data centers of a business or other organization, not made available to the general public, when they are large enough to benefit from the advantages of cloud computing that we discuss here.The cloud computing is the sum of SaaS and utility computing, but does not include medium sized data centers, even if these depend on virtualization for management. People can be users or providers of SaaS, or users or providers of utility computing. We focus on SaaS providers (cloud users) and cloud providers, which have received less attention than SaaS users. Figure 1 makes provider-user relationships clear. There are some case in which the same actor plays multiple roles. For

DOI : 10.5121/ijcsit.2012.4202

instance, a cloud provider might alsohost its own customer-facing services on cloud infrastructure.[1]

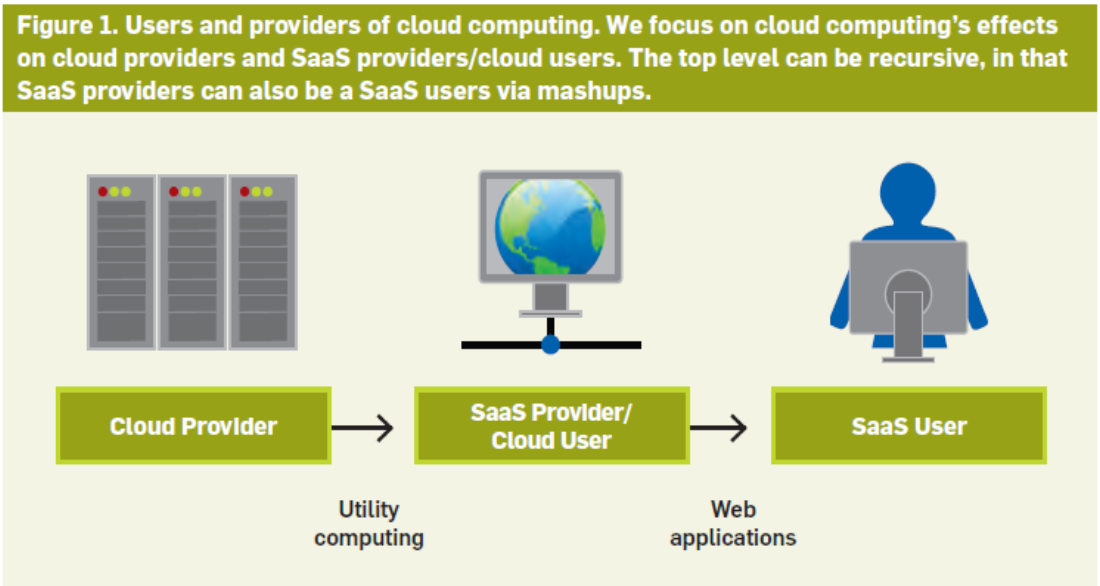

Figure 1

1.2 All kinds of clouds

Major IT companies have spent billions of dollars since the 1990s to shape cloud computing. Like, Sun's well-known slogan "the network is the computer" was made in 1980s. Salesforce.com is the website which has been providing on-demand Software as a Service (SaaS) for customers since 1999 to present era. IBM and Microsoft are the first two companies that started to deliver Web services in the early 2000s. Microsoft's Azure service provides an operating system and a set of developer tools and services. Google's popular Google Docs software provides Web-based word-processing, spreadsheets and all the Microsoft office applications. Google App Engine allows system developers to run their Python/Java applications on Google's infrastructure. Sun provides $1 per CPU hour. Amazon is well-known for providing Web services such as EC2 and S3. Yahoo! announced that it would use the Apache Hadoop framework to allow users to work with thousands of nodes and petabytes (1 million gigabytes) of data.

These examples demonstrate that cloud computing providers are offering services on every level, from different hardware (e.g., Amazon and Sun), to the different operating systems (e.g., Google and Microsoft), to software and different services (e.g., Google, Microsoft, and Yahoo!). At present era Cloud-computing providers target a variety of end users, from developers of the software to the general public. For additional information regarding cloud computing models, the University of California (UC) Berkeley's report provides a good comparison of these models by Amazon, Microsoft, and Google[2]. As cloud computing providers prices are low and IT advancements remove technology barriers—such as virtualization ,simulation , network bandwidth — cloud computing has moved into the mainstream of technology .[3] Gartner stated, "Organizations are switching from company-

owner hardware and software to per-use service-based models."[4] For example, the U.S. government website (http://www.usa .gov/) will soon begin using cloud computing.[5] The *New York Times* used Amazon's EC2 and S3 services and used Hadoop application to provide open access for the public domain articles from 1851 to 1922. The *Times* loaded 4 TB of raw TIFF images on web and their derivative 11 million PDFs into Amazon's S3 in twenty-four hours at very less cost.[6] This project is very similar to digital library projects run by academic libraries. Few years ago OCLC announced its movement of library management services to the Web.[7] It is clear that OCLC is going to deliver a Web-based integrated library system (ILS) on web for enhancing the technology to provide a new way of running an ILS. Dura Space, a joint organization by Fedora Commons and D Space Foundation, announced that they would be taking advantage of cloud storage and cloud computing.[8]

2. Delivery Models of Cloud Computing

The NIST [10] definition of cloud computing defines three delivery models:

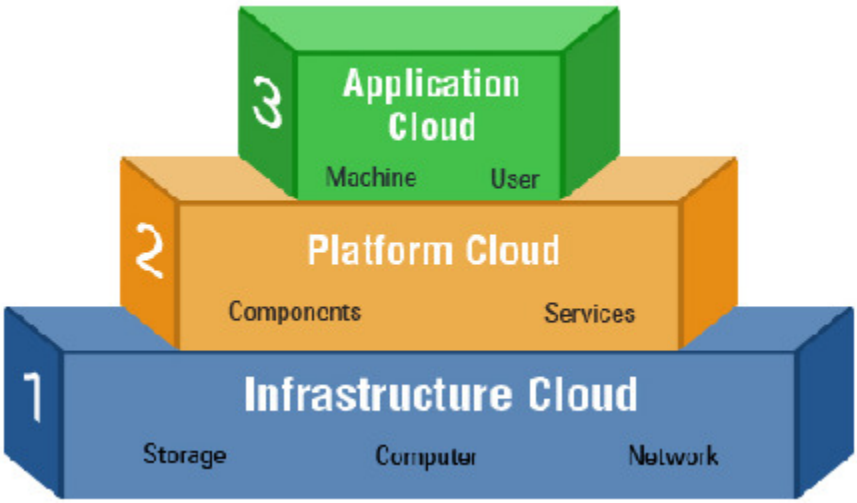

Figure 2

2.1. Software as a Service (SaaS)

The consumer uses an application, but does not control the operating system, hardware or network infrastructure on which it's running. The SaaS model shown in the diagram admits that the provider manages the entire suite of applications delivered to end-users. SaaS providers are responsible for securing these applications. Customers can be normally responsible for operational security processes. However the following questions, along with other sections within this document, should assist in assessing their offerings:

• Administration controls are provided by them and can these be controls used to assign read and write privileges to other users?

• SaaS access control is quite fine grained and can be customized to ones organizations policy?

2.2. Platform as a Service (PaaS)

The consumer uses a hosting environment for their applications. The consumer controls the applications that run in the environment (and possibly has some control over the hosting

environment), but does not control the operating system, hardware or network infrastructure on which they are running. The platform is typically an application framework. Generally speaking, PaaS service providers are responsible for the security of the platform software stack, and the recommendations throughout this document is a good foundation for ensuring a PaaS provider has considered security principles before designing and managing their PaaS platform. It is very difficult to get or obtain the detailed information from PaaS providers on exactly how they secure their platforms however there are some of the following questions that should be along with other sections within these document.

- A high level description of containment and isolation measures is required for request information on how multi-tenanted applications are isolated from each other.
- What assurance can the PaaS provider give by which the data can be accessed?
- Does the provider ensure that the PaaS platform sandbox is monitored for new bugs, new attactks and vulnerabilities?

2.3. Infrastructure as a Service (IaaS)

The consumer uses “fundamental computing resources” such as processing power, storage, networking components or middleware. The consumer can control the operating system, storage, deployed applications and possibly networking components such as firewalls and load balancers, but not the cloud infrastructure beneath them., Many of the potential issues with personnel security arise because the IT infrastructure is under the control of a third party like traditional outsourcing, multiple customers get effect because of a physical security breach.

- What assurance can be provided to the customer regarding the physical security of the location?
- Who has unescorted access to IT infrastructure? For example, vendors’, managers, physical security staff, contractors, consultants, cleaners, etc.
- How often are access rights reviewed?
- How quickly can access rights be revoked?
- Does the security risks are assessed and parameters evaluated on a regular basis?
- How frequently?
- Are regular risk assessments being done which may include things such as neighboring buildings?
- Is access secure areas controled or monitored personnel (including third parties)?
- What are the policies/procedures that are used for loading, unloading and installing equipment?
- When are processes or procedures required to destroy old media or systems?
- Data overwritten?
- Physical destruction?
- How often are checks made to ensure compliance with the environment with the appropriate legal and regulatory requirements of a organization[11][9].

3. Different Cloud Computing's Architecture

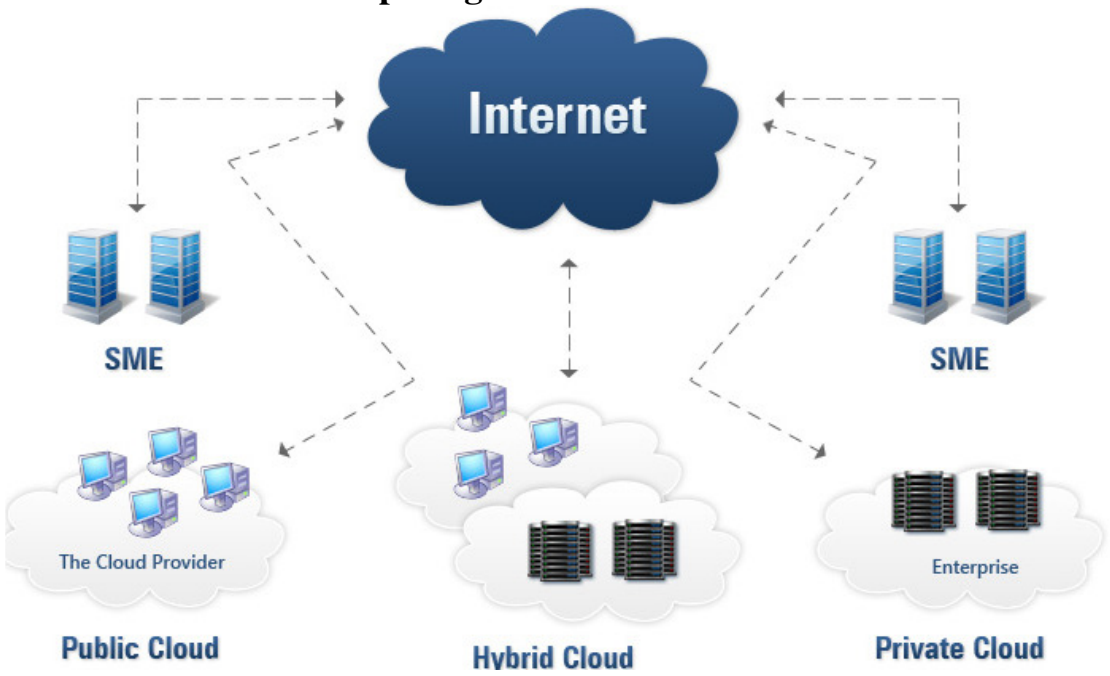

Figure 3[21]

• **Public Cloud: A** public cloud is a standard cloud computing model wherein a service provider manages storage and computing resources on behalf of consumer over the Internet.

The term "public cloud" arose to differentiate between the standard model and the private cloud, which runs on proprietary network or data center of the user. Public clouds are run by third parties, and applications from different users are shared on the provider's cloud servers, storage systems, and networks. Public clouds are most often hosted away from customer premises, and they try to reduce customer risk and cost by substituting their enterprise infrastructure.

Applications which are required for temporary purpose or for short duration are the best suitable for deployment in a public cloud because it avoids the need to purchase additional equipment to solve a temporary need.

• **Private Cloud:** Private cloud (also called internal cloud or corporate cloud) is typically hosted on customer premises. With proprietary computing architecture, it provides hosted services to authorized users behind a company firewall. Thus company has control over resources, data, security and QoS.

The company owns the infrastructure and controls how applications are deployed on it. Private clouds can be deployed in an organization datacenter or also at a collocation facility. Company's own IT department or cloud service provider can built and manage private clouds. In this type of cloud computing, a company can install, configure, and

operate the infrastructure as per its requirement and demand. A permanent application, or one that has specific requirements on quality of service or location of data, is most suitable to deploy in a private or hybrid cloud. Company's own IT department uses their own private clouds for critical and other secured systems deployments [21]

• **Hybrid cloud** is a cloud computing infrastructure composed 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[22] In hybrid cloud architecture, companies and individuals can obtain degrees of fault tolerance combined with locally immediate usability without internet connectivity. y Hybrid Cloud architecture is the ideal combination that requires on premises resources and off site (remote) server based cloud infrastructure. Hybrid clouds do not have the flexibility, security and certainty of in-house applications.[23]

4. Security Issues in Private Cloud Computing

Due primarily to the security concerns associated with the public cloud, many firms have elected to favor private cloud deployments over public clouds. While security pros are on their guard when it comes on private cloud. Private cloud gives more control to in house staff, but increased control cannot ignore the security. On the other hand, there are some security risks associated with all cloud models, private included. Because of security pros are less sensitive to risks and the control is high in the private model.

4.1 Comingled regulatory environments

Security cannot be fitted in every situation of IT environment. For example, that an entity regulated under PCI would find a non PCI certified environment is unacceptable for systems which are in cardholder data environment. This is true for both the public and private cloud. An infrastructure is dedicated to be used alone does not mean everything can go with equal ease. Because private cloud grants greater control over regulatory compliance and security, the security should always be given the forefront of planning, particularly when multiple types of regulated data are in play, such as a customer data, comingled mix of payment card data and sensitive business intelligence.

4.2 Viability of security tools

When an organization virtualizes a physical host it always needs to evaluate how network aware tools will be impacted. If visibility into traffic can be impacted: network IDS and sniffers. For example, consider an n-tier Web application with separate Web, application and DB servers that attach to one switch that is monitored by IDS. If these three devices are moved to virtual slices on a hypervisor, traffic will no longer visible on the wire, which will cause the IDS to lose visibility. At one time particularly true when large numbers of hosts are virtualized; more number of hosts' means less time spent planning per host.

4.3 Data expansion

Cloud is a fantastic enabler of resource centralization. For example, a virtualized environment can allow far-flung resources to come together under an environment. However, if resources are centralized, data becomes denser. While this its a boon for management, it is challenging from security standpoint, particularly when considering tools are being used that operate across

the data in aggregate. Antimalware scanning, bulk encryption and data discovery tools required that when we have a harder time dealing very large amounts of data. Existing tools should be examined to determine what impact they have on data volumes increase and new tools are considered when operation would be impacted severely and old tools are ineffective.

4.4 Future proofing

Private cloud does not means "on-premise," but some may think that way. The defining aspect of private cloud is about which are users that use the infrastructure, not who maintains the infrastructure. So it is not necessarily many private cloud deployments will use on-premise infrastructure. And even if a deployment uses on-premise or dedicated resources today, that cannot prevent it from migrating off-premises to use a service provider or onto shared infrastructure. Organizations that put into a private environment today can easily migrate tomorrow. So private cloud deployments have many security advantages. A private cloud deployment is every bit as serious as a move to public cloud and needs to be planned for accordingly.**[14]**

4.5 Fear of change.

IT team may not be familiar with the term private clouds, so because of that there will be a big learning curve. There can also be new operational processes and some of old processes that need much of the rework. To turn this into a growth opportunity for people, the stress of doing and learning all this can be mitigated by helping your collogues keep in mind that these are important new skills in today's business environment.**[15]**

5. Issues in Public Cloud Computing

5.1 Third-Party Risk

SaaS will effectively manage the security risks with third parties if SaaS moves into cloud computing for the storage and processing of customer data. Poor third-party risk management program may result in damage to provider's reputation, revenue losses, and legal actions should the provider be found not to have performed due poor activity on its third-party vendors **[19]**

5.2 Security & Compliance

Because of data security issues associated with the public cloud, all the mid-size and large enterprises overwhelmingly prefer private clouds because of network. HIPAA Compliance or PCI Compliance cannot be achieved in a public cloud.

5.3 Data Loss – No High Availability Fail Over –

One of the Amazon's cloud crashes while wiping out their customers data and their impersonal response to their customers. If a host crashes, all of the virtual servers and data of the user on that hardware host gets lost. Public cloud servers cannot provide high availability or automatic fail over.

5.4 Fraud & Spammers

One public cloud hosting provider can have fraud rates as high as 80%. Fraudulent users can spin up a cloud server because sign up & deployment is fast & easy, a fraudulent user can spin up a cloud server on a stolen credit card, launch attacks and can be easily gone invisible before

the credit card fraud is found. Because of another user's is if the shared server hardware is seized in any condition under warrant fraud the only concern for legitimate users.

Not all the applications are good fit for the public cloud. Many mid-size and large enterprises that want to assure the security & safety of their corporate clients and client data will move to the private cloud and cannot deploy their critical systems in the public cloud. However, there are a number of applications that are ideal for public cloud hosting including:

5.5 Development & Test Environments

Regression testing is a great example of an application for the public cloud. In past, in software development life, spend dozen servers to run thousands of test scenarios every 24 hours. With the ability to have 1000's of servers programmatically, the test time can be reduced to only a few minutes, it speeds up software development cycles.

5.6 Compute Intensive Research Applications

At the University of Michigan Ann Arbor, Michigan in the United States, researchers are spending 1000's of cores to run their DNA, weather analysis programs and genome. Many of these programs are developed to withstand the crash of a server or two, so the public cloud with spot demands pricing can provide tremendous resources that are very cost effectively for research computing.

5.7 Noncritical Web Servers

These are those applications where a loss of data or crash of the server isn't critical from the organization's point of view.

6. Cost Comparison Over 3 years without depreciation

This cloud comparison is based on some assumptions of course. There are various factors that could go into any implementation, however for discussion purposes; I think this is a good starting point. For the purpose of this financial analysis, assumptions are following:

Assumed all instances of Public or Private Cloud server usage can be active 24/7.

- Calculated the Public Cloud (Option 1) using the, 10 Extra Large CPU classes, 30 Small CPU classes and 60 Large CPU classes.
- For initial analysis purposes here are used about scenario of 100 virtual server instances.
- For the Private Cloud, included a Silver level support in the costing scenario.
- Included all needed servers, storages, switching and software infrastructure which come under the Private Cloud scenario.
- Over a three year period(Examined all scenarios) with an assumed 15% growth rate in server instances (Public Cloud scenario) and virtual server deployment (Private Cloud scenario).
- Allocated support cost yearly they occur & allocated maintenance.
- Determined the company's technical staff proficiency and if they had the skills to install and configure this infrastructure themselves, which can decreased the cost as

company did not included the professional services to install all the the Private Cloud infrastructure.

It also includes costs for racks, power, space, etc. at a co-located data center facility in the Private Cloud scenario, using a quote for a 24 month commitment approximately at a local datacenter co-location facility. Additionally, we procured a quote for a Phoenix co-lo that had higher initial one-time costs with a lower monthly charge. But we can determine that the benefits of having local access to the equipment out-weighed the monthly charges which was low before. Over a three year period the difference between the two proposals is approximately $2,000.**[17]**

	Year 1	**Year 2**	**Year 3**	**Cumulative**
Option 1: Public Cloud				
Capital Expense	$ -	$ -	$ -	$ -
Operating Expenses	$ 314,525.00	$ 361703.75	$ 415959.31	$ 1,092,188.06
TOTAL	**$ 314,525.00**	**$ 361703.75**	**$ 415959.31**	**$ 1,092,188.06**
Option 2: Private Cloud Purchase				
Capital Expense	$315,446.94	$ -	$ -	$ 315,446.94
Operating Expenses	$ 90,948.80	$86,248.80	$86,248.80	$ 263,446.40
TOTAL	**$ 406,395.74**	**$ 86,248.80**	**$ 86,248.80**	**$ 578,893.34**
Option 3: Private Cloud Lease				
Capital Expense	$ -	$ -	$ -	$ -
Operating Expenses	$203,904.80	$199,204.80	$ 199204.80	$ 602,314.40
TOTAL	**$203,904.80**	**$199,204.80**	**$199,204.80**	**$ 602,314.40**

Table1

This table shows the Cost Comparison over 3 years without depreciation

7. Cost Breakdown of Public vs Private Cloud Computing

In an application the cost or the seat also varies greatly by the type (class). The classes of application, as defined in previous work by Wikibon, are as follows: Class 1 – Development, File & Print, Small Data Marts, Small-scale applications & Data Base servers

1. Class 2 – Medium-scale applications & DB servers, Data Marts, Small CRM, Small Data Warehouses, Messaging (Exchange, etc)
2. Class 3 – Mission Critical Applications, Enterprise CRM, ERP, Large scale OLTP, Large scale DB Servers, Large Scale messaging

3. Class 4 – Large-scale applications requiring highest levels of availability, security & recoverability **[18]**

The following diagram gives a cost breakdown of class 3 application of an organization with greater than $1B in revenue or budget

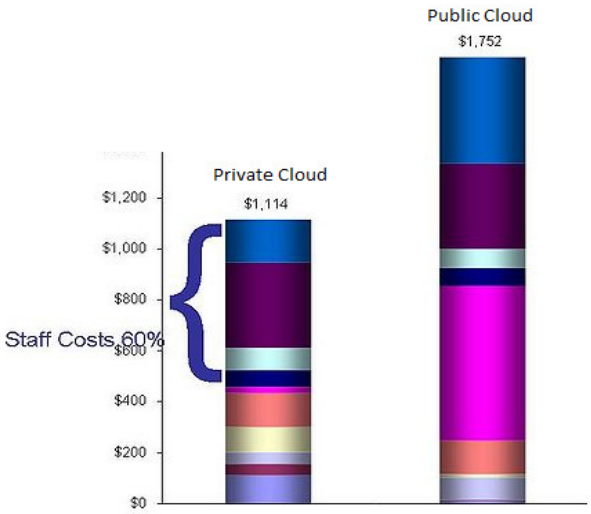

Figure 4

Figure 4: This figure shows the Cost Breakdown of Public vs Private Cloud Computing of class 3.

	Priavte Cloud	Public Cloud
Management Costs (Executive, Audit, Security)	$167	$418
Development Staff Costs	$334	$334
Operational Staff Costs	$89	$76
Help Desk Costs	$67	$67
Outsourcing Costs	$22	$609
Application Software Costs	$134	$134
Infrastructure Software	$100	$10
Network Infrastructure & Management Costs	$45	$89
Storage Infrastructure Hardware, Maintenance, Facilities etc.	$45	$4
Server Infrastructure Hardware, Maintenance, Facilities, etc.	$111	$11
Total	$1,114	$1,752

Table2

Table 2: This table shows the Cost Breakdown of Public vs Private Cloud Computing of class 3.

The key points the data illustrates are:

- 60% of the private cloud costs are labor, and 40% are associated with equipment.
- There are limited labor savings when transferring to the private cloud.
- To manage today's public cloud, for class 3 applications with high integrity, security and audit requirements there would significantly increased management, audit and the cost of the security. In order to maintain higher levels of security and audit can be offered by Future offerings, and would shift some of the labor cost to the subscription costs
- Network and network management would be more complex and costs would be significantly higher in a public cloud setting

7.1Cloud Computing Usage and Why are you considering the use of public cloud computing and private cloud computing.

Which of the following best describe your organization's adoption of private cloud computing and public cloud computing.

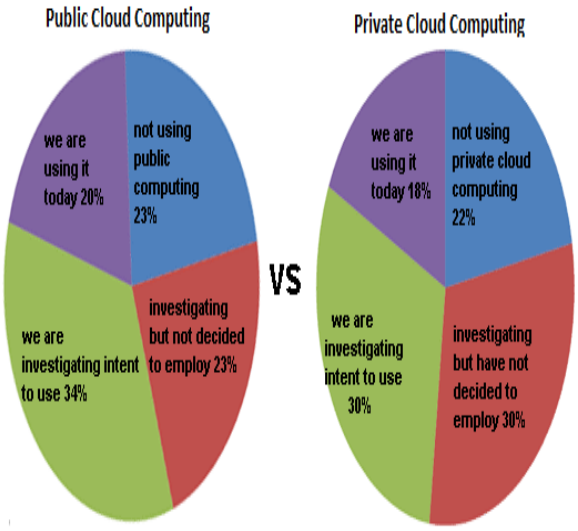

Figure 5

Figure 5 This figure provides the cloud computing usage in the big Organizations.

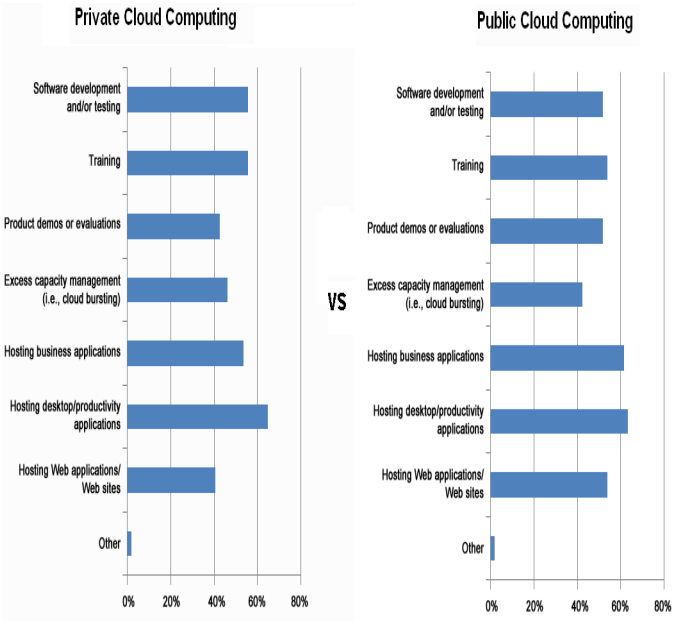

Figure 6

Figure 6 This figure provides the people opinion about why they use private and public cloud computing

7.2 Cloud Computing Spending Upon 2010 and 2011

The "mean" is the "average" you're used to, where you add up all the numbers and then divide by the number of numbers. The "median" is the "middle" value in the list of numbers. To find the median, your numbers have to be listed in numerical order, so you may have to rewrite your list first. The "mode" is the value that occurs most often. If no number is repeated, then there is no mode for the list.**[20]**

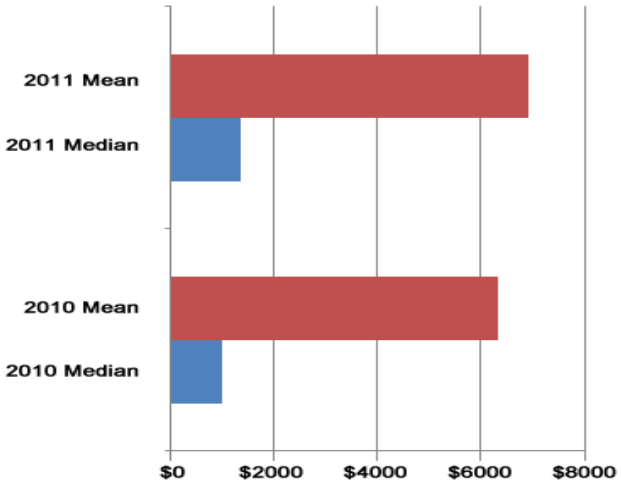

Figure 7

8. CONCLUSION

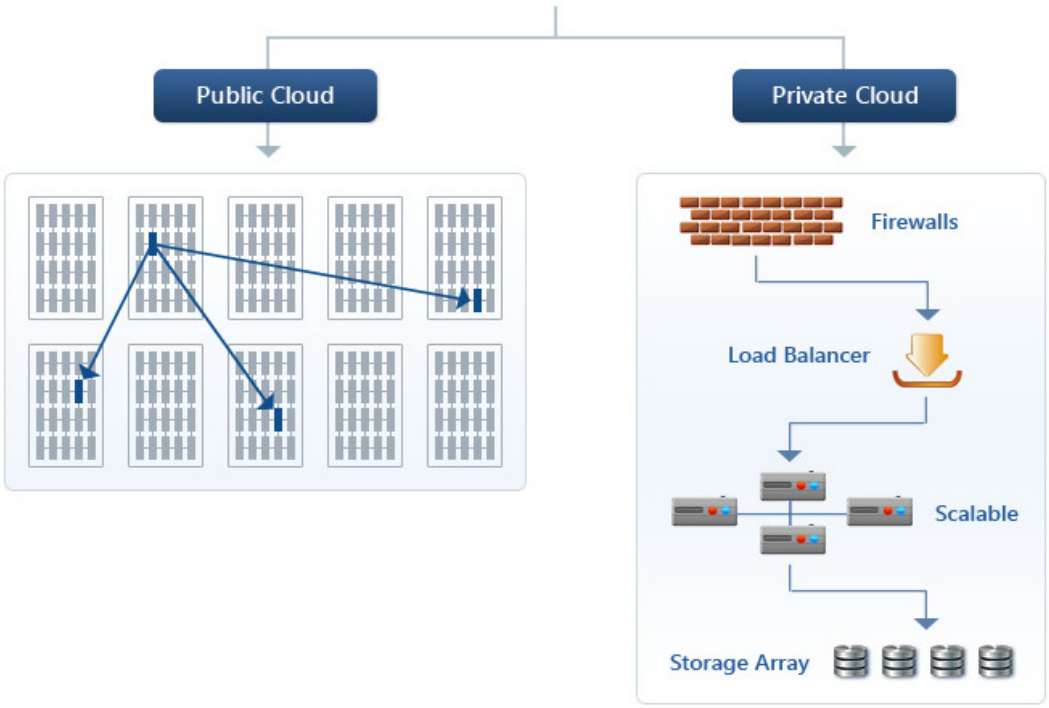

Figure 8: It describes the main Conclusion that which cloud computing is suitable for the organization according to the need.

- Developing a strategic plan for virtualization will evolve into private or public computing, including your future virtualization architecture.
- Private cloud computing is a major investment. Although issues with privacy and security can be real with public cloud computing services, before you rule out using public cloud computing services test your assumptions and fully analyze your requirements.
- Before investing in technology solutions private cloud computing requires a vivid focus on people issues (cultural and political) and process issues (operational, management, funding and service description).

9. REFRENCES

[1] Michael Armbrust, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy Katz, Andy Konwinski, Gunho Lee, Dav id Patterson, Ariel Rabkin, Ion Stoica, and Matei Zaharia "Clearing the clouds away from the true potential and obstacles posed by this computing capability" communications of the ac m | april 2010 | vol. 53 | no. 4

[2] Michael Armbust et al., "Above the Cloud computing: A Berkeley View of Cloud Computing, "technical report, University of California, Berkeley, EECS Department,Feb. 10, 2009, http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.html .

[3] Eric Hand, "'Cloud Computing' Is Being Pitched as a New Nirvana for Scientists Drowning in Data. But Can It Deliver?" *Nature* 449,no. 7165 (2007): 963; Geoffrey Fowler and Ben Worthen, "The Internet Industry Is On a Cloud very soon—Whatever That May Mean," *Wall Street Journal*, Mar. 26,2009, http://online.wsj.com/article/SB123802623665542725.html (accessed July 14, 2009); Stephen Baker, "Google and the Wisdom of the Clouds," *Business Week* (Dec. 14, 2007), http://www.msnbc.msn.com/id/22261846/ .

[4] Gartner, "Gartner Says Worldwide IT Spending on Pace to Supass $3.4 Trillion in 2008," press release, Aug. 18,2008, ttp://www.gartner.com/it/page.jsp?id=742913 .

[5] Wyatt Kash, "USA.gov, Gobierno USA.gov move into the Internet cloud, *"Government Computer News*, Feb. 23, 2009,http://gcn.com/articles/2009/02/23/gsa-sites-to-move-to-the-cloud.aspx?s=gcndaily_240209.

[6] Derek Gottfrid, "Self-Service, Prorated Super Computing Fun! "online posting, New York Times Open, Nov. 1, 2007, http://open.blogs.nytimes.com/2007/11/01/self-service-prorated-super-computing-fun/?scp=1&sq=self%20service%20prorated&st=cse .

[7] OCLC Online Computing Library Center, "few years ago OCLC announces strategy to move library management services to Web scale," press release, Apr. 23, 2009,http://www.oclc.org/us/en/news/releases/200927.htm .

[8]. DuraSpace, "Fedora Commons and DSpace Foundation Join Together to Create DuraSpace Organization," press release, May 12, 2009, http://duraspace.org/documents/pressrelease.pdf .

[9] The European Network and Information Security Agency (ENISA), "Cloud Computing: Benefits, Risks and Recommendations for Information

[10] NIST, January 2010. http://www.nist.gov/

[11] P. Mell and T. Grance, "Effectively and Securely: Using the cloud computing Paradigm," NIST, Information technology Laboratory, Boulder, December 2009.

[12]Michael Vizard, Public Versus Private Cloud Distinction Starts to Blur available on: http://www.itbusinessedge.com/cm/blogs/vizard/public-versus-private-cloud-distinction-starts-to-blur/?cs=45246

[13]Tom bittman, The Spectrum of Private to Public Cloud Services *:* avialabe on: *http://blogs.gartner.com/thomas_bittman/2009/04/08/the-spectrum-of-private-to-public-cloud-services*

[14] Ed Moyle ,Private cloud computing security issues http://searchcloudsecurity.techtarget.com/tip/Private-cloud-computing-security-issues

[15] Bill Claybrook | Computerworld US | available on: http://features.techworld.com/data-centre/3236805/private-cloud-builders-need-to-prepare-for-problems

[16] Mike Klein,Three Benefits of Public Cloud Computing Available on on http://resource.onlinetech.com/three-benefits-of-public-cloud-computing/

[17]Available on : http://blog.virtual.com/2011/private-vs-public-cloud-computing-solutions-financial-comparison\

[18]David Floyer , Private Cloud is more Cost Effective than Public Cloud for Organizations over $1B Available on : http://wikibon.org/wiki/v/Private_Cloud_is_more_Cost_Effective_than_Public_Cloud_for_Organizations_over_$1B

[19] Swarnpreet singh , Ritu bagga, "Challenges among Public Cloud Computing " SUS National Conference on Advance Computer Trends. Page 23 issue 5 Decemeber 2011

[20] Stapel, Elizabeth. "Mean, Median, Mode, and Range." Purple math. Available on: http://www.purplemath.com/modules/meanmode.htm

[21] "Private v/s Public Cloud – Which one is for me?" Friday, August 12, 2011. Available from: http://www.tatvasoft.com/blog/2011/08/enterpise-application-public-private-cloud.html

[22] Peter Mell Timothy Grance "A NIST Definition of Cloud Computing". National Institute of Science and Technology. NIST Special Publication 800-145 Retrieved 21 October 2011.

[23] Alan Stevens" When hybrid clouds are a mixed blessing". Posted in Data Centre, 29th June 2011 10:00 GMTFree whitepaper – 2011 Lippis Report .Available from: *http://www.theregister.co.uk/2011/06/29/hybrid_cloud/*