INTERNATIONAL JOURNAL OF R&D IN ENGINEERING, SCIENCE AND MANAGEMENT vol.1, issue III, Oct.2014
p.p.84-93, ISSN 2393-865X

INTERNATIONAL JOURNAL OF R&D IN ENGINEERING SCIENCE AND MANAGEMENT

Cloud Computing Paradigms and Challenges

Hawa Singh

Assistant Professor, Department of CSE, St. Margaret Engineering College, Neemrana, India

ABSTRACT

Although cloud computing has recently attracted significant momentum and attention in both academia and industry users. This is due to noticing drastic change in everyone's perception of infrastructure availability, software delivery and development models. Representing the step by step deployment from mainframe computers to cloud computing architecture, following the transition throw personal computer, network, client / server, internet and grid computing models. This rapid change towards the cloud computing, has fuelled on this critical issue for the success of information systems, communication and information security. To words the perspective of security, a number of risks and challenges have been introduced regarding relocation to the cloud computing, deteriorating much of the effectiveness of traditional protection mechanisms.

As a result the aim of this paper is firstly to introduce some of the paradigm towards cloud computing, application, advantage and drawbacks of cloud computing and secondly to evaluate cloud security by identifying some of the challenges in the cloud computing. The aim of this paper is to provide a better understanding of cloud computing and identifying security requirements in the cloud computing model.

Keywords: Paradigms, Advantages, Drawbacks, Challenges.

1. Introduction

Cloud computing is receiving great deal of attention in both kind of users, individual at home and users at organizations. Cloud computing is a subscription based service provided by respective service provider to use networked storage space and computer resources according to your requirement. Provider takes care of housing all of the hardware and software necessary to support user's personal requirement. When user want to access his data he just have to open web browser, go to the server of the service provider, and log in as a client.

Fig.1 illustrates the computing paradigm shift of the last half century [8]. The figure shows six distinct phases. In Phase1, user uses terminals to connect to powerful mainframes shared by many users. Terminals were basically little more than keyboards and monitors. In Phase2, stand-alone personal computers (PCs) became powerful enough to satisfy users requirements. Phase3 provides computer networks that allowed multiple computers to connect to each other [8]. You could work on a PC and connect to other computers through local networks to share resources. Phase 4 shows the advent of local networks that could connect to other local networks to establish a more global network called Internet; users could now connect to the Internet to utilize remote applications and resources. Phase 5 brought us the concept of an electronic grid to facilitate shared computing power and storage resources (distributed computing). People used PCs to access a grid of computers in a transparent manner. Now, in Phase 6, cloud computing let us exploit all available resources on the Internet in a scalable and simple way [7].

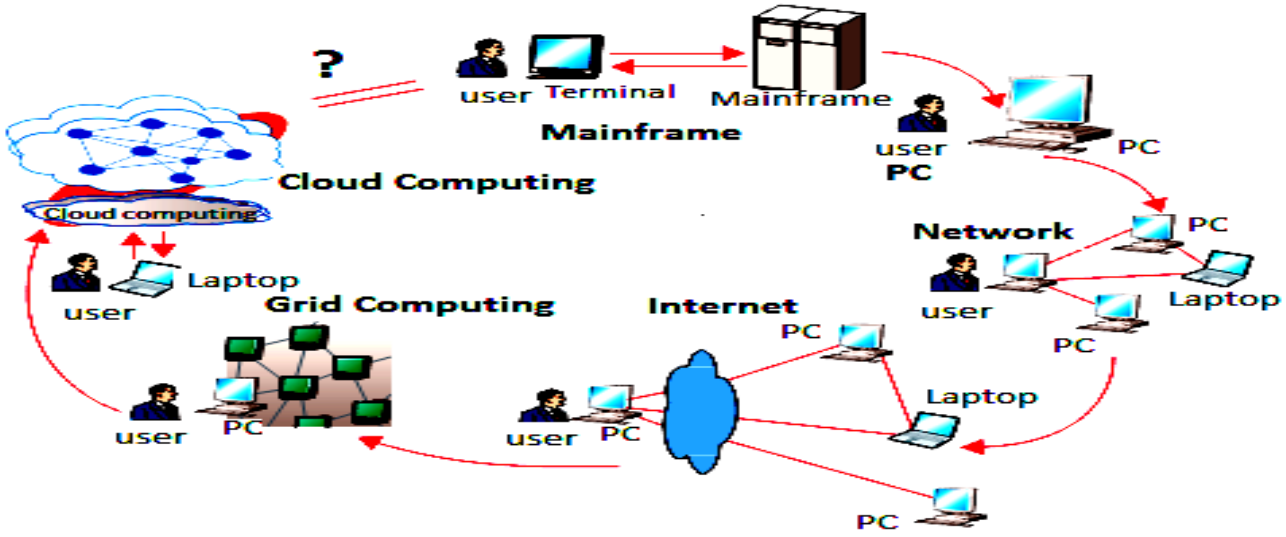

Fig. 1 – Computing paradigm shift over six distinct phases, computers evolved from dummy terminals to grids and clouds [8]

As Fig.1 shows, a conceptual layer—a cloud on the Internet—hides all available resources (hardware or software) and services, but it publishes a standard interface. As long as users connecting to the Internet, they have the entire cloud services just as their power PC. Cloud computing thus refers to the techniques that enable and facilitate this kind of scenario [7, 8].

The most important part of the whole process is to have internet access. You can access all your data and information anywhere and at any time through an internet connection. Cloud provider establishes both hardware and software necessary to run your both kind of (home or business) applications. This is especially helpful for businesses that cannot afford the large amount of hardware and storage space as like in big company. Small companies can store their information in the cloud, reducing the cost of purchasing and storing memory devices [8]. Additionally, because you only need to buy the amount of storage space as per your requirement, an organization can purchase more space or reduce their subscription as their business grows or as they find that they need less storage space [8].

Fig. 2 – Computing paradigm

So our main requirement is that, user need to have an internet connection in order to access the cloud. This means that if user wants to look at a specific document which is housed in the cloud, user must first establish an internet connection either through a wireless or wired internet or a mobile broadband connection [8]. The benefit is that use can access the required information from anywhere and on any device (desktop, laptop, tablet, and phone etc) that can access the internet. This can also help your business to

function more smoothly because anyone who can connect to the internet and have right to access your cloud can work on data, access software, and store data in the cloud. This is the freedom that the cloud can provide for you or your organization.

1.1. Types of Clouds

On the basis of subscriber, there are different types of clouds. Depending on subscriber's needs and services any one of these can subscribed.

1. **Public Cloud -** A public cloud can be accessed by any subscriber with an internet connection and access to the cloud space [8].
2. **Private Cloud -** A private cloud is established for a specific group or organization and limits access to just that group [8].
3. **Community Cloud -** A community cloud is shared among two or more organizations that have similar cloud service requirements [8].
4. **Hybrid Cloud -** A hybrid cloud is essentially a combination of at least two clouds, where the clouds included are a mixture of public, private, or community type of clouds [8].

As a home user or small business owner, subscribers will most likely use public cloud services.

1.2 Types of cloud provider

On the basis of the service provided by the cloud provider, there are three types of cloud providers that you can subscribe to [8]:

1. Software as a Service (SaaS)
2. Platform as a Service (PaaS)
3. Infrastructure as a Service (IaaS)

These three types differ in the amount of control that you have over your information available in your cloud, and conversely, how much your provider can do for you. Briefly, here is what you can expect from each type [7, 8].

Software as a Service

- SaaS provider gives subscribers access to both resources and applications.
- SaaS allows you to install software on your device without having a physical copy of software.
- SaaS also allows having the same software on all of your devices by accessing it from cloud.
- In a SaaS agreement, you have the least control over the cloud.

Platform as a Service

- A PaaS system goes a level above the Software as a Service setup.
- In PaaS agreement, subscribers allows to access all the components that they require to develop and operate applications over the internet

Infrastructure as a Service

- An IaaS agreement, as the name states, deals primarily with computational infrastructure.
- In an IaaS agreement, the subscriber completely outsources the storage and resources, such as hardware and software that they need.

Each provider provides some specific services, giving more or less control to the users over their cloud depending on the type user requested or paid for. When you choose a provider, compare your needs with the available services of the cloud. Your cloud needs will vary depending on how you intend to use the space and resources associated with the cloud. If it will be for personal home use, you will need a different cloud type and provider than if you will be using the cloud for business. Keep in mind that your cloud provider will be pay-as-you-go, meaning that if your technological needs change at any point you can purchase more storage space (or less for that matter) from your cloud provider [7,8].

As we move from top to down the list from number first to number three, the subscriber gains more control over what they can do within the space of the cloud. The cloud provider has less control in an IaaS system than with SaaS agreement. It means user can choose its level of control on the basis of information and types of services that user want from a cloud provider. However, this system may mean user have to spend more of its resources on the development and operation of applications. It allows the users to evaluate its current computational resources, the level of control he want to have, financial situation, and where he foresee his business going before signing up with a cloud provider. If use is a home user, however, user will most likely be looking at free or low-cost cloud services (such as web-based email) and will not be as concerned with many of the more complex cloud offerings. After having fully taken stock of where you are and where you want to be, research into each cloud provider, it will give you a better idea of whether it is is right for you or not [4].

2. Applications of Cloud Computing

In just few years, cloud computing has transformed from an interesting buzzword into the future of the Internet due to its application. These are few most common cloud computing applications cases illustrating our point of view on where we'll see the cloud having the biggest impact in computer society [4].

2.1. File Storage and Sharing

Many users, many times have suffered the frustration of trying to send or receive a very large file via email. Services like SendFile, Dropbox and Rackspace's own JungleDisk have been around for years. Many researchers are helping the industry by explaining the concept of the cloud to the general population. Cloud computing brings you mature and powerful options for secure file sharing for workgroups, team collaboration and file storage and backups. From Cloud Drive to hosted SharePoint, there is no reason to send large attachments anymore. Your virtual team, including partners and customers, can have a place in the cloud where they share information and documents [4].

2.2. Cloud Database

Almost every web application needs a database. In the past, web developers had to set up and maintain their own databases: MySQL, SQL Server, etc. Managing and tuning a database requires a very specific skill set to perform complex tasks. This work is best done by a database administrator. Cloud databases give developers and IT a powerful and scalable database that just works. From the infrastructure to the database software to the tuning and monitoring everything is done as a service. Rackspace offers multiple options: from a web application platform that includes database functions to a fully managed database server to cloud based solutions from partners such as Xeround [4,5].

2.3. CRM

Companies are adopting the cloud computing for mission critical applications. Customer Relationship Management (CRM) systems are mission critical and deal with two of the most sensitive pieces of data: customer information and revenue. Yet, most companies don't even consider hosting their CRM applications on premise. There are many websites for CRM over the last few years. The advantages of cloud-based CRM systems are clear for Sales teams and IT and the risks have been addressed. CRM can become a blueprint for moving more line of business applications to the cloud [5].

2.4. Email

Email is another mission critical application that is fairly mature and standardized, prime to move to the cloud. For years, CIOs have expressed a desire to outsource email. After cloud it makes no sense to host an Exchange server under a desk at a company of any size. Independent professionals to large multinational companies should move their email to the cloud as soon as possible. At a personal level, we all use cloud-based consumer email services like Hotmail and Gmail, and we enjoy the benefits of access anywhere and not having to think about capacity or server uptime. There is a right cloud email solution for every business, be it hosted low-cost email, Hosted Exchange for small businesses, or even managed dedicated Exchange environments for large customers [4].

2.5. PaaS for Web Applications

Platform as a Service (PaaS) became a buzzword in last few years. Like many buzzwords, it is probably overhyped, yet there is real value in the concept of a PaaS. A PaaS solution allows developers to host their applications without having to think about servers at all: they just upload their application and it runs. The caveat is that the application 'stack' is a black box that has predefined components and settings. This makes a PaaS, like Cloud Sites, ideal for web developers, micro sites and stand alone applications that don't need stack customizations and don't interact with other line of business applications [4,5].

2.6. File Backup

Everyone should be backing up all important documents and files, but few of us actually do it consistently and efficiently. A good backup stores a copy of your files at a remote location. Until recently, that meant making a backup to a disk or tape and shipping those to a storage facility which was logistically complex, time consuming and not very cost effective. Cloud-based backup is a powerful solution: backups can be scheduled to run automatically, information is stored in a secure remote location where it will always be available when needed and capacity is never a problem [5].

2.7. Web Site Hosting

Websites can be a huge drain on IT resources, especially if the websites are visited frequently. Hosting the website in the cloud combined with managed services allow web teams to focus their efforts on creating the best web content possible (instead of sweating the ins and outs of web hosting). From a simple blog site to a high trafficked corporate website, cloud-based web hosting can provide scalability and high availability when designed properly [5].

2.8. eCommerce

Scalability and availability are critical concerns for online stores. Every minute of downtime can result in lost sales. A slow website can result losing a customer for life. eCommerce is also known for seasonal high peaks, such as the holiday season. Online stores no longer have to pay for and deploy infrastructure to support peak times, the cloud allows them to dynamically scale as their traffic scales. When a spike in interest at an eCommerce website occurs, the demand could bring down or significantly slow down traditional servers, preventing customers from being able to make a purchase. However, the cloud allows that same website to quickly spin up additional resources and handle the load. When the rush subsides, those resources are turned off. The cloud also makes it easy to deploy web servers in different locations with load balancing to accelerate local page load times and increase availability. Adding the services of a Content Delivery Network (CDN) makes it easy to distribute high-bandwidth content like images and video across the world in a very efficient and cost effective way [5].

2.9. Test & Development

A software company that is deploying a new line of business software, or building a software application to sell in the market, usually requires two or more 'QA environments' – each one being a setup of servers, storage and networking. Instead of buying and maintaining these QA environments, software development teams can create them in the cloud. Development teams will benefit from the agility of creating instances in minutes, the efficiency of paying only for the infrastructure needed at any given point in time and from the efficiency of not having to manage and maintain the infrastructure. Additional instances can be set for testing and training purposes with the same efficiency. Load testing and simulation under different hardware configurations is also a no-brainer for the cloud [5].

2.10. Private and Hybrid Clouds

Private clouds give IT departments many of the benefits of the public cloud with the added benefit of having an isolated network and computing resources that bring additional security. Rackspace offers private clouds that give IT departments a lot

more control over the resources deployed and the architecture. Hybrid clouds, enabled by technologies such as Rack Connect™, allow IT departments to connect public cloud, private cloud, dedicated hosted and on-premise infrastructure to gain the optimum combination of control and agility. For example, a web server can be set up in the public cloud, transaction processing can be in a dedicated server where PCI compliance is easier to attain, order processing can be on-premise and the ERP system can be on a private cloud with automatic backups going to storage on the public cloud. The cloud is not a go/no-go decision for IT departments and small businesses; however, the thinking should be about how to maximize the value of the cloud. It is hard to find a consumer, small business or IT department that does not use the cloud in some shape or form [5].

3. Benefits of Cloud Computing

There are many benefits of using cloud computing, but these three are the main:

3.1 Reduces cost

There are many reasons that proves that cloud computing is cost effective. The billing model will be as per the uses; as the infrastructure is not purchased by user thus there is no maintenance cost. Initial expense and recurring expense are much lower than traditional computation [8].

3.2 Increased Storage

With the massive Infrastructure that is offered by Cloud providers, storage & maintenance of large volumes of data can be achieved easily. Sudden workload spikes are also managed effectively & efficiently, since the processing and storage capacity of cloud can be scale dynamically [8].

3.3 Flexibility

This is an extremely important characteristic. With enterprises having to adapt, to changing business conditions, speed to deliver even more rapidly is critical. Cloud computing stresses service provider, to get applications in market, very quickly, by using the most appropriate building blocks necessary for deployment [8].

4. Drawbacks of Cloud Computing

4.1 Possible downtime

Cloud computing makes the small business dependent on the reliability of Internet connection. When it's offline, you're offline. If internet service suffers from frequent outages or slow speeds cloud computing may not be suitable for your business. Even the most reliable cloud computing service providers suffer server outages now and again [7, 8].

4.2 Security issue

How safe is your data? Cloud computing means, Internet computing. So you should not be using cloud computing applications that involve using or storing data that you are not comfortable having on the Internet. Established cloud computing vendors have gone to great lengths to promote the idea that they have the latest, most sophisticated data security systems possible as they want your business and realize that data security is a big concern; however, their credibility in this regard has suffered greatly in the wake of the recent scandals. Keep in mind also that your cloud data is accessible from anywhere on the internet, meaning that if a data breach occurs via hacking, a disgruntled employee, or careless username/password security, your business data can be compromised. Leaving aside revelations about the NSA, switching to the cloud can actually improve security for a small business, says Michael Redding, managing director of Accenture Technology Labs. "Because large cloud computing companies have more resources, he says, they are often able to offer levels of security an average small business may not be able to afford implementing on its own servers" [7, 8].

4.3 Cost

At first glance, a cloud computing application may appear to be a lot cheaper than a particular software solution installed and run in-house, but you need to be sure you're comparing apples and apples. Does the cloud application have all the features that the software does and if not, are the missing features important to you? You also need to be sure you are doing a total cost comparison. While many cloud computer vendors present themselves as utility-based providers, claiming that you're only charged for what you use, Gartner says that this isn't true; in most cases, a company must commit to a predetermined contract independent of actual use. To be sure you're saving money; you have to look closely at the pricing plans and details for each application [8]. In the same article, Gartner also points out that the cost savings of cloud computing primarily occur when a business first starts using it. SaaS (Software as a Service) applications, Gartner says, will have lower total cost of ownership for the first two years because SaaS applications do not require large capital investment for licenses or support infrastructure. After that, the on-premises option can become the cost-savings winner from an accounting perspective as the capital assets involved depreciate. Cloud computing costs are constantly changing, so check current pricing [8].

4.4 Inflexibility

Be careful when you're choosing a cloud computing vendor that you're not locking your business into using their proprietary applications or formats. You can't insert a document created in another application into a Google Docs spreadsheet, for instance. Also make sure that you can add and subtract cloud computing users as necessary as your business grows or contracts.

4.5 Lack of support

There are some issues need to be resolved before using cloud computing services (OPEN Forum). Customer service for Web apps leaves a lot to be desired -- All too many cloud-based apps make it difficult to get customer service promptly – or at all. Sending an email and hoping for a response within hours is not an acceptable way for most of us to run a business [7].

5. Cloud Computing Challenges

Despite its growing influence, concerns regarding cloud computing still remain. In our opinion, the benefits outweigh the drawbacks and the model is worth exploring [1].

5.1 Data Protection

Data Security is a crucial area which warrants scrutiny. Enterprises and individual users are reluctant to buy an assurance of business data security from vendors. They fear losing data to competitor and the data confidentiality of consumers [2]. In many cases, the actual storage location is not disclosed, adding onto the security concerns of enterprises. In the existing models, firewalls across data centers (owned by enterprises) protect this sensitive information. In the cloud model, Service providers are responsible for maintaining data security and enterprises would have to rely on them [2].

5.2 Data Recovery and Availability

All business applications have Service level agreements that are stringently followed. Operational teams play a key role in management of service level agreements and runtime governance of applications. In production environments, operational teams support appropriate clustering and fail over, data replication, system monitoring (Transactions monitoring, logs monitoring and others), maintenance (Runtime Governance), disaster recovery, and capacity & performance management if, any of the above mentioned services is under-served by a cloud provider, the damage & impact could be severe [2].

5.3 Management Capabilities

Despite there being multiple cloud providers, the management of platform and infrastructure is still in its infancy. Features like "Auto-scaling" for example, is a crucial requirement for many enterprises. There is huge potential to improve on the scalability and load balancing features provided today [2].

5.4 Regulatory and Compliance Restrictions

In some countries, Government regulations do not allow customer's personal information and other sensitive information to be physically located outside the state or country. In order to meet such requirements, cloud providers need to setup a data center or a storage site exclusively within the country to comply with regulations. Having such an infrastructure may not always be feasible and is a big challenge for cloud providers. With cloud computing, the action moves to the interface — that is, to the interface

between service suppliers and multiple groups of service consumers. Cloud services will demand expertise in distributed services, procurement, risk assessment and service negotiation — areas that many enterprises are only modestly equipped to handle [1].

5.5 Network Security

In the past, network have often been misused for placing malware which is then used to send spam, or their processing power has been exploited to crack passwords using brute force attacks, or to hide command and control servers used to control botnets. To prevent these attacks as well as the misuse of resources, proper and effective security measures to be taken against network-based attacks. Because of the concentration of resources in centralized data centers, an attack which is a particular threat to public Cloud Computing platforms is the Distributed Denial of Service (DDoS) attack. A standard backbone is designed for a far lower data rate. As a result, many CSPs can hardly defend against DDoS attacks using high data rates. This can have serious consequences for both the victim themselves and other connected customers. As Cloud Computing platforms consist of many different components, the overall configuration is very complex. Changing a configuration parameter for one component (e.g. virtualization server) can, when interacting with other components (e. g. network or storage) lead to security vulnerabilities, faulty functions and/or failures. For this reason the components deployed need to be securely and carefully configured. All CSPs should also ensure that their networks are suitably segmented, preventing any faults from spreading freely. In this context the option exists to define and set up different security zones within the provider's network, based on the protection requirement [1, 2].

- Security zone for managing the cloud
- Security zone for the live migration, if server virtualization is being used
- Security zone for the storage network
- With IaaS, customer to have their own security zones for the virtual machines

The CSP's management network should be isolated from the data network. If the cloud infrastructure or cloud services are being administered remotely, this needs to be accomplished via a secure communication channel (e.g. SSH, TLS/SSL, IPSec, VPN). If a consumer has particularly high availability requirements in terms of the services they are drawing down, the CSP's sites should be networked on a mutually redundant basis [6].

5.6 Encryption and key management

To store, process and transport sensitive data securely, suitable cryptographic methods and products should be used. The management of cryptographic keys in Cloud Computing environments is complex, and there are currently no appropriate tools for key management. For this reason, most providers do not encrypt data however, the customer has the option of encrypting their data themselves prior to storage. In this way, they retain complete control over the cryptographic keys and also obviously need to deal with key management. If the provider encrypts the data, suitable security measures should be implemented at each phase in a cryptographic key's life cycle to ensure that keys are generated, stored, shared, used and destroyed on the basis of confidentiality, integrity and authenticity. The following key management best practices should be implemented [3].

- Keys should be generated in a secure environment and using suitable key generators.
- Where possible, cryptographic keys should be used for one purpose only.
- In general, keys should never be stored in the system in a clear form, but always encrypted. Furthermore, the storage always be redundantly backed up and restorable, to avoid losing a key.
- The keys must be distributed securely (on the basis of confidentiality, integrity and authenticity).
- The cloud's administrators should have no access to customers' keys.
- Keys should be changed regularly. The keys used should be regularly checked to ensure they are current.
- Access to key management functions should require a separate authentication.
- The keys should be archived securely.

- Keys that are no longer required (e.g. keys whose validity duration has elapsed) should be deleted or destroyed in a secure manner.

Adequate cryptography skills are required for reliable key management. For this reason, CSP personnel who are responsible for key management must be identified and trained [4].

6. Security issues in Cloud Computing

The information stored on the cloud is seen very valuable to individual with malicious intent. There is a lot of personal information and potentially secure data that people stores on their computers, and this information is now being transferred to the cloud. This makes it critical for consumer to understand the security measures that cloud provider has in place, and it is equally important to take personal precautions to secure the data. The first thing consumer must look into is the security measures that the cloud provider already has in the cloud [1]. These vary from provider to provider and among the various types of clouds. What encryption methods do the providers have in place? What methods of protection does the cloud have for the actual hardware in which data will be stored? Will they have backups of the data stored on cloud? Do they have firewalls set up? If you have a community cloud, what barriers are in place to keep individuals information separate from other companies? Many cloud providers have standard terms and conditions that may answer these questions, but the home user will probably have little negotiation room in their cloud contract [1,2].

A small business user may have slightly more room to discuss the terms of their contract with the provider and will be able to ask these questions during that time. There are many options that consumer has to check, but it is important to choose a cloud provider that considers the security of the data as a major concern. No matter how careful the use is with is personal data, by subscribing to the cloud it will be giving up some control to an external source. This distance between user and the physical location of the data creates a barrier. It may also create more space for a third party to access your information [2]. However, to take advantage and benefits of the cloud, use will have to knowingly give up direct control of data. On the converse, keep in mind that most cloud providers will have a great deal of knowledge on how to keep the data safe. A provider likely has more resources and expertise than the average user to secure their computers and networks [2].

7. Conclusions

The cloud provides many have options for the everyday computer user as well as large and small businesses. It opens up the world of computing to a broader range of uses and increases option to use fast and efficient resources by providing cloud access through any internet connection [1]. However, with the increase in facility, drawbacks also come. User has less control over who has access to the information and ahs no information that where it is stored. Consumer also must be aware of the security risks of having data stored on the cloud. The cloud is a big target for malicious individuals and may have disadvantages because it can be accessed through an unsecured internet connection [8].

If users are going to use the cloud, be certain that it must be identified what information you will be putting in the cloud. Who will have access to that information, and what will need to make sure it is protected [8]. Additionally, know the options in terms of what type of cloud will be best for once needs, what type of provider will be most useful for that type of consumer, what the reputation and responsibilities of the providers and what kind of challenges are available with the cloud type and with the cloud provider you are considering, before select the cloud provider for you [7, 8].

REFERENCES

[1]. Dimitrios Zissis, Dimitrios Lekkas (2010) 'Addressing Cloud Computing Security Issues', *Future Generation Computer Systems*, Vol. 28, No.3 pp. 583 – 592.

[2]. Qi Zhang, Lu Cheng and Raouf Boutaba 'Cloud Computing: Sate-of-the-art and research challenges', The Brezilian Computer Society,Springer, Published online, 2010.

[3]. Lizhe Wang, Gregorvn Laszewski, Marcel Kunze and Jie Tao, Cloud computing: A Perspective study, in: Proceedings

of the Grid Computing Environments (GCE) workshop, held at the Austin Civic Centre, Texas, 2008, pp. 2-11.

[4]. Frahan Bashir Shaikh and Sajjad Haider, 'Security Threats in Cloud Computing', 6th International Conference on Internet Technology and Secured Transactions, at Abu Dhabi, United Arab Emirates, on December 2011, pp. 214 - 219.

[5]. Hosam AlHakami, Hamza Aldabbas and Alwada'n (2012), 'Comparison Between Cloud and Grid Computing: Review Paper', *International Journal on Cloud Computing Services and Architecture (IJCCSA)*, Vol. 2, No.4, pp. 1 – 21.

[6]. Anthony Bisong and Syed M. Rahman (2011), 'An Overview of the Seccurity Concerns in Enterprise Cloud Computing', *International Journal of Network Security and Its Applications (IJNSA)*, Vol. 3, No.1, pp. 30-45.

[7]. Cong Wang, Qian Wang, Kui Ren and Wenjing Lou, 'Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing', in: Proceedings of the IEEE Communications Society subject matter experts for publication in the IEEE INFOCOM, 2010,pp. 1-10.

[8]. Jeffrey Voas and Jia Zhang, 'Cloud Computing New Wine or Just a New Bottle?' Guest Editors' Introduction in: IT Pro magazine Published by IEEE Computer Society. 2009, pp. 15-17.