Is Cloud Computing the Undisputed New Era Computing? -- A Comprehensive Analysis.

Aishwarya Iyer
FCRIT (University of Mumbai)
Vashi, Maharashtra, India
aishuiyer2001@yahoo.com

***Abstract*—Cloud computing is the latest technology used for implementing business applications. Instead of running your apps yourself, they run on a shared data center. Cloud computing is Internet based computing where virtual shared servers provide software, infrastructure, platform, devices and other resources and hosting to customers on a pay-as-you-use basis. Cloud-based apps can be up and running in days or weeks, and they cost less. It's not just a fad—the shift from traditional software models to the Internet has steadily gained momentum over the last 10 years. However, corporate executives might hesitate to take advantage of a cloud computing system because they can't keep their company's information under lock and key. Cloud computing customers do not own the physical infrastructure, rather they rent the usage from a third-party provider. Many enterprises look at cloud computing warily due to projected security risks. The risks of compromised security and privacy may be lower overall with cloud computing than they would be if the data were to be stored on individual machines. Cloud computing is amongst today's hot technologies due to its ability to reduce costs associated with computing while increasing flexibility and scalability for computer processes. In this paper we will be discussing the concept of cloud computing, its characteristics, applications and future scope. The security issues and privacy concerns along with risk management have also been put forth.**

***Keywords*: Cloud computing, services, characteristics, security, risk management, applications, trends, future scope.**

I. INTRODUCTION

Cloud computing is a marketing term for technologies which provide computation, software, data access, and storage services that do not require end-user knowledge of the physical location and configuration of the system delivering the services .It describes highly scalable computing resources provided as an external service via the internet on a pay-as-you-go basis. The cloud is simply a metaphor for the internet, based on the symbol used to represent the worldwide network in computer network diagrams. Economically, the main appeal of cloud computing is that customers only use what they need, and only pay for what they actually use. Resources are available to be accessed from the cloud at any time, and from any location via the internet. Because of this, cloud computing has also been called utility computing, or 'IT on demand'. This might lead to a confusion between the terms 'utility computing' and 'cloud computing'. So to get a clear picture, we can say that Utility Computing is not a new paradigm of computing infrastructure; rather, it is a business model in which computing resources like computation and storage, are packaged and offered as metered services. This may be considered similar to a physical public utility, such as electricity and public switched telephone network. Utility computing is typically implemented using other computing infrastructure (e.g. Grids) with additional accounting and monitoring services. A Cloud infrastructure can be utilized internally by a company or exposed to the public as utility computing. There are a set of important policy issues in Cloud computing technology, which include issues of privacy, security, anonymity, telecommunications capacity, government surveillance, reliability, liability etc. But the most serious issue is considered to be security and how the cloud provider assures it. Cloud computing may have customers from varying fields. Each of them may have a different motive for moving to the cloud. The cloud provider must be able to satisfy each one's need without compromising on security at any level.

II. CHARACTERISTICS OF CLOUD COMPUTING AND TYPES OF CLOUDS

A. Cloud computing characteristics.

Cloud computing exhibits the following key characteristics:

1) Service On demand: The Cloud is a huge pool of resources where you buy only what you need. Cloud is just like any metered service like running water or electricity wherein you are charged only for the amount you use.
2) High scalability: The scale of cloud can extend dynamically to meet the increasing requirement. Scalability and Elasticity via dynamic ("on-demand") provisioning of resources on a self-service basis near real-time, without users having to engineer for peak loads is a typical characteristic of this system.
3) Reliability: This is improved if multiple redundant sites are used, which makes well-designed cloud computing suitable for business continuity and disaster recovery. Cloud uses data multi-transcript fault tolerant, the computation node isomorphism exchangeable and so on to ensure the high reliability of the service [2]. Using cloud computing is more reliable than local computer.
4) Versatility: Cloud computing doesn't aim at certain special application. It can produce various applications supported by cloud, and one cloud can support different applications running it at the same time. Performance is monitored, and consistent and loosely coupled architectures are constructed using web services as the system interface [2].
5) Security: It could improve due to centralization of data, increased security-focused resources, etc., but concerns can persist about loss of control over certain sensitive data, and the lack of security for stored kernels. Security is better than other traditional systems, in part because providers are able to devote resources to solving security issues that many customers cannot afford. However, the complexity of security is greatly increased when data is distributed over a wider area or greater number of devices and in multi-tenant systems that are being shared by unrelated users. In addition, user access to security audit logs may be difficult or impossible. Private cloud installations are in part motivated by users' desire to retain control over the infrastructure and avoid losing control of information security.

B. Types of cloud computing

Cloud computing is typically classified in two ways:

1. Location of the cloud computing
2. Type of services offered

1. Location of the cloud.

Cloud Computing can be classified into 4 types on the basis of location where the cloud is hosted:
a) Public Cloud: A public cloud is based on the standard cloud computing model, in which a service provider makes resources, such as applications and storage, available to the general public over the Internet [1]. Public cloud services may be free or offered on a pay-per-usage model. Computing infrastructure is hosted at the vendor's premises. The customer has no visibility over the location of the cloud computing infrastructure.
b) Private Cloud: Here, computing architecture is dedicated to the customer and is not shared with other organizations. They are expensive and are considered more secure than Public Clouds. Private clouds are of two types: On-premise private clouds and externally hosted private clouds [3]. Externally hosted private clouds are exclusively used by one organization, but are hosted by a third party specializing in cloud infrastructure. Externally hosted private clouds are cheaper than On-premise private clouds. Private cloud is infrastructure operated solely for a single organization, whether managed internally or by a third-party and hosted internally or externally. However, some experts consider that private clouds are not real examples of cloud computing.
c) Hybrid Cloud: Hybrid cloud is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together, offering the benefits of multiple deployment models. It can also be defined as multiple cloud systems that are connected in a way that allows programs and data to be moved easily from one deployment system to another.
d) Community Cloud: The cloud infrastructure is shared between the organizations of the same community. For example, all the government agencies in a city can share the same cloud but not the non-government agencies. Community cloud shares infrastructure between several organizations from a specific community with common concerns, whether managed internally or by a third-party and hosted internally or externally. The costs are spread over fewer users than a public cloud (but more than a private cloud), so only some of the cost savings potential of cloud computing are realized.

2. Classification of Cloud on the basis of service provided

a) Infrastructure as a Service (IAAS): Hardware related services are provided using the principles of Cloud Computing. These include disk storage and virtual servers. IaaS allows an organization to run entire data center application stacks, from the operating system up to the application, on a service provider's infrastructure.
b) Platform as a service (PAAS)**:** PaaS offerings facilitate deployment of applications without the cost and complexity of buying and managing the underlying hardware and software and provisioning hosting capabilities, providing all of the facilities required to support the complete life cycle of building and delivering web applications and services entirely available from the Internet. These services may be provisioned as an integrated solution over the web. Google App Engine, Microsoft Azure and Saleforce's force.com are the leaders in this category. PaaS involves providing a platform on which a customer can run its own applications.
c) Software as a service (SAAS)**:** This is the most common form of cloud computing. It is a complete software offering on the cloud. They are accessed by the customers on pay per use basis. Salesforce.com's CRM, Gmail and Hotmail are prime examples of SAAS. Companies buy access to an

application but have no responsibility for (and no control over) its implementation.

III. RISK MANAGEMENT : CLOUD COMPUTING CONSIDERATIONS

In a troubled economy, Cloud Computing becomes a great cost saving alternative. Google, Microsoft, IBM and all other cloud providers provide cloud services as a major cost saving alternative to the traditional data centers, which can be extremely compelling. But like everything that's too good to be true, Cloud Computing comes with its own set of risks which must be well recognized before making the plunge. Hence, it's very essential to understand the risks and then have a mitigation strategy for each.

a) Who accesses your sensitive data: The physical, logical and personnel controls are no longer under your control when you move your organization's information on the cloud. The cloud provider maintains his own hiring practices, rotation of individuals, and access control procedures. It's important to ask and understand the data management and hiring practices in place with your cloud provider.

b) Regulatory Compliance: You are answerable to your customers for any security and integrity issues that may affect your data. The ability of the cloud provider to mitigate your risk is typically done through a process of regular external audits, PEN tests, compliance with PCI standards, ensuring SAS 70 Type II standards to name a few. You are responsible to weigh the risks to your organization's information and ensure that the cloud provider has standards and procedures in place to mitigate them.

c) Geographical spread of your data**:** Your data may not be residing in the same city, state or country as your organization. While the provider may be contractually obliged to you to ensure the privacy of your data, they may be even more obliged to abide by the laws of the state, and or country in which your data resides. So your organization's rights may get marginalized. Ask the question and weigh the risk.

d) Data loss and recovery: Data on the cloud is almost always encrypted; this is to ensure security of the data. However, this comes with a price – corrupted encrypted data is always harder to recover than unencrypted data. It's important to know how your provider plans to recover your data in a disaster scenario and more importantly in how much time. The provider must be able to demonstrate bench-marked scenarios for data recovery in a disaster scenario.

e) What happens when your provider gets acquired: A seamless merger/acquisition on the part of the cloud provider is not common business for his client. The provider should have clearly acknowledged and addressed this as one of scenarios in their contract. Is there an exit strategy for the client – and what are the technical issues he could face to get his data into someplace else?

f) Availability of data**:** The cloud provider relies on a combination of network, equipment, application, and storage components to provide the cloud service. If one of these components goes down, you won't be able to access your information. It's important to weigh your tolerance level for unavailability of your information against the vendors guaranteed up-time.

IV. APPLICATIONS OF CLOUD COMPUTING

The applications of cloud computing are practically limitless. With the right middleware, a cloud computing system could execute all the programs a normal computer could run. Potentially, everything from generic word processing software to customized computer programs designed for a specific company could work on a cloud computing system.

Why would anyone want to rely on another computer system to run programs and store data? Here are just a few reasons:

– Clients would be able to access their applications and data from anywhere at any time. They could access the cloud computing system using any computer linked to the Internet. Data wouldn't be confined to a hard drive on one user's computer or even a corporation's internal network.

– It could bring hardware costs down. Cloud computing systems would reduce the need for advanced hardware on the client side. You wouldn't need to buy the fastest computer with the most memory, because the cloud system would take care of those needs for you. Instead, you could buy an inexpensive computer terminal. The terminal could include a monitor, input devices like a keyboard and mouse and just enough processing power to run the middleware necessary to connect to the cloud system. You wouldn't need a large hard drive because you'd store all your information on a remote computer.

– Corporations that rely on computers have to make sure they have the right software in place to achieve goals. Cloud computing systems give these organizations company-wide access to computer applications. The companies don't have to buy a set of software or software licenses for every employee. Instead, the company could pay a metered fee to a cloud computing company.

– Servers and digital storage devices take up space. Some companies rent physical space to store servers and databases because they don't have it available on site. Cloud computing gives these companies the option of storing data on someone else's hardware, removing the need for physical space on the front end.

– Corporations might save money on IT support. Streamlined hardware would, in theory, have fewer problems than a network of heterogeneous machines and operating systems.

– If the cloud computing system's back end is a grid computing system, then the client could take advantage of the entire network's processing power. Often, scientists and researchers work with calculations so complex that it would take years for individual computers to complete them. On a grid computing system, the client could send the calculation to the cloud for processing. The cloud system would tap into the processing power of all available

computers on the back end, significantly speeding up the calculation.

V. SECURITY ISSUES AND TRENDS

Top issues of Cloud services are security, performance, and availability. These are all good concerns and need to be addressed. Performance and availability are big issues because as soon as you move your services from your environment where you can touch and feel things to out there literally in the Cloud, there could be some impact. An enterprise moving a legacy application to a cloud computing environment gives up control over the networking infrastructure, including servers, access to logs, incident response and patch management [7]. You're giving that over to someone else who's providing it for you. While that can have extraordinary cost savings and removes the administrative burden, it also moves the level of control way up the stack. In your infrastructure, you understand what's happening. In this case, you don't know. It's just a cloud managed by someone else and they may not be willing to share with you how things are set up. It must be made sure that Service Level Agreements (SLAs) from Cloud providers are very clear on these issues. The key security issues from customers' point of view seem to be around security defects in the technology itself, unauthorized access to customer information, encryption, application security, identity management, virtualization security etc.

Responsibility for security issues depends on which tier of cloud offering is being used. So, for IaaS, vendor responsibility is around physical, environmental, and virtualization security. Every other aspect of security in applications, operating system, etc. still needs to be handled by the customer. On the other hand if a SaaS offering is being used, the vendor is responsible for all elements of security [7]. The key issues to keep in mind are stated below:

- Physical Security – You want to make sure that physical security around the infrastructure is very tight – even tighter than in your environment because it's not your employees anymore.
- Insider Abuse – When you "cloudize" your environment, you lose control over who's managing that infrastructure with your confidential information. Insider abuse is a common problem where information can be stolen and passed on to outsiders or they can collude with hackers.
- Data Encryption – Cloud environments are shared and your data is in the same environment alongside data from other customers. Breaches can easily happen from one database to another.
- Third party Relationships – You are as strong as your weakest link. And, in corporate environments, your weakest link could be your integration with your partners. In case of Cloud providers, this is even more important due to integrations of various third parties and applications into the Cloud environment.
- Network Security – In the recent months, aggressive marketing by various Cloud providers have made it easier for hackers to get accounts and plant botnets. Cloud is also susceptible to a lot more Denial of Service attacks. Cloud Providers need to ensure that their perimeter is secure and barrier to attacks is high.
- Virtualization Security – Almost all Cloud providers use virtualization to provide economies of scale and optimal distributed architecture. Virtualization has its own set of security issues.
- Access Controls – Some of the big issues for Cloud services are around access control, authentication, user management, provisioning etc.
- Application Security – With over 75% of attacks happening through Web applications, this becomes a critical piece in the overall cloud decision making process. Although the exposure is similar to what you would have in your own environment, it's on a massive scale and you may not have any control over it.

VI. FUTURE SCOPE

The future of cloud computing is expected to see lot of technological advances with a scope to change the world. The advancement in cloud computing will use applications which will extract entire potential of the cloud. But it will only be well known when it is used with Internet having higher bandwidth rates and can be accessed at faster speeds because many of the public places like airlines, educational institutions now have hotspots which have wireless internet facilities. The future of cloud computing also shows that the burden of maintaining software in client's computer will be negligible since there is no need to install the software application on their computer so there will no need for the person to take stress for maintenance or troubleshooting issues if any arises. The applications can be operated on by using an interface designed especially for cloud computing which will make it easier for the person to access the software which is installed on one specific computer in a network. If the software can be accessed over web browser, then there will be minimal need to store data on the computer which indirectly points to another advantage offered by the future of cloud computing where the end user will not have to invest large amounts of money to buy hard disks which can store loads of information in various formats and types. All the data is stored safely on internet along with ready backup all the time. For people who are a lot into gaming, future of cloud computing assures them that with the reduced usage of hardware, there will be no chance of virus entering the system since everything will be operated over the network and using web browser. The future of cloud computing shows scope for many areas of fields like medicine, education and space where there is need for larger storage spaces and which requires high bandwidth internet which might seem difficult if the system does not use cloud computing. Cloud computing reduces the cost and risks of having storage area

.It can have the data stored readily with backup without the need to do it manually.

VII. CONCLUSION

Though cloud computing is relatively new in its current form, it definitely can be applied to specific low to medium risk business areas. Given that it's relatively new, there is no clear cut template for success. You can only minimize your risk but rewards can be tremendous if the risks are well managed. The privacy and security risks associated with this model must be weighed against alternatives. Don't hesitate to ask the questions, and if necessary, engage an independent consulting company that can guide you through the process. Picking your cloud provider requires far more due diligence than routine IT procurement. Cloud computing systems are normally designed to closely track all system resources, which enables providers to charge customers according to the resources each consumes. Some customers will prefer this so-called metered billing approach to save money, while others will prefer a flat-rate subscription to ensure predictable monthly or yearly costs. Cloud Computing offers many benefits. Although Security is a big issue, it should not scare you away from using the Cloud that can save you a lot of money and resources. The key is to do proper due diligence with your Cloud Providers and really understand their Service Level Agreements (SLAs). Ask the right questions and take your time in selecting the right provider for you based on your requirements and risk appetite. You should definitely jump on this exciting car ride. But do make sure you are secure with your seatbelt on.

REFERENCES

[1] http://en.wikipedia.org/wiki/Cloud_computing

[2] Shuai Zhang , Xuebin Chen, Shufen Zhang, Xiuzhen Huo," Cloud Computing Research and Development Trend", 2010 Second International Conference on Future Networks.

[3] Chunye Gong, Jie Liu, Qiang Zhang, Haitao Chen and Zhenghu Gong, "The Characteristics of Cloud Computing",2010 39th International Conference on Parallel Processing Workshops.

[4] Shubhashis Sengupta, Vikrant Kaulgud, Vibhu Saujanya Sharma, "Cloud Computing Security - Trends and Research Directions", 2011 IEEE World Congress on Services.

[5] On the future technology trends: the development of cloud computing security, http://stor.zol.com.cn/128/1288536.html, April 13, 2009(reproduced).

[6] Farzad Sabahi, "Cloud Computing Security Threats and Responses"

[7] T. Velte, A. Velte, and R. Elsenpeter, Cloud Computing Basics, 1st ed., McGraw-Hill Osborne Media, Sept.2009.