Fear of Cloud

Vinnakota Saran Chaitanya[1], G. Harshavardhan Reddy[2]

[1] UG Final year student, Department of Computer Science and Engineering, G. Pulla Reddy Engineering College, Andhra Pradesh, India
[2] UG Final year student, Department of Electronics and Communication Engineering, Manipal Institute of Technology, Karnataka, India

---***---

ABSTRACT: Cloud Computing is the latest technology which helps organizations to store their large amounts of data without bothering about the underlying architecture. The paper starts from the very basic definition of cloud, its various forms and importance. However the paper realizes the importance of the word "TRUST" in the context of cloud computing which do not have any mathematical formula. However the paper addresses the security issues or fears and their relation with the word trust.

Keywords: Trust, Multi tenancy, Pay per use billing and Clipper chip.

I. Introduction:

Data has been tremendously increasing from Bytes, Kilobyte, Megabyte, Gigabyte, Terabyte, Peta byte, Exabyte, Zeta byte and Yota byte. A lot of infrastructure is needed to maintain this amount of huge data. This leads to a lot of expenses, in maintaining it. Cloud is a technology which helps in storage of data without bothering about the underlying architecture. As per National Institute of Standards and Technology [NIST] cloud computing may be defined as "Cloud Computing is a model for enabling ubiquitous, convenient, on demand network access to a shared pool of configurable computing Resources that can be rapidly provisioned and released with minimal management effort (or) service provider interaction".

II. Cloud Architecture

NIST'S five essential characteristics of cloud computing provide enough specifics to break the myth that "The Internet Equals the cloud". Neither simple web hosting nor virtualized data centers deliver the following comprehensive cloud benefits.

1. On-demand self service: The service provision storage and processing power as needed without customer interaction with service provider.
2. Broad Network Access: Clients access the service using web browsers (or) through applications.
3. Resource Pooling: Customers share pooled computing resources and data storage cloud customers may specify where to store data at a macro level (Such as geographical region), but they will not know exact location of their application (or) data storage.
4. Rapid Elasticity: The storage, network band width and compute capacity available to a service can be increased or reduced almost immediately allowing solutions to be scaled for optimal resource usage.
5. Measured Service: Cloud systems can measure transactions and use of resources plus they can monitor, control and report usage in transparent way.

Thus measured service is nothing but the "Pay Per Use" billing method, similar to our electricity billing.

Let us take computational users as well as the computation needs:

1. As end user/gadget user I need application software that will run my application.
2. As business man I need to popularize my website (or) business I need Infrastructure such as server software etc…
3. As a developer I need a platform to develop my software.

Thus cloud computing provides services to all the above said, three kinds of computational needs. These are nothing but the service delivery models. Thus Infrastructure as a Service, Platform as a Service and Software as a Service are the three service delivery models which provide service to business user, developers and end users respectively. As per NIST these three are standard service delivery models that are to be possessed by any of the cloud. There are many other service delivery models such as Business Platform as a service (BPASS) etc…

IaaS: IaaS is used to run client or server applications on virtual machines. The cloud provider manages the network, servers and storage resources so that IT managers or any other clients need not to buy, track or decommission hardware.

PaaS: The PaaS is used to develop, deploy, monitor & maintain applications while the cloud provider manages everything else, including as OS and middle ware. Developers can manage configuration remotely with IAAS but they need not build and configure VM image themselves. Overall PaaS lowers total cost of ownership than IaaS.

SaaS: SaaS is perhaps the most familiar service delivery model, in which companies subscribe to prepackaged applications that run on cloud infrastructure & allow access from a variety of devices.

Examples of the service providers:

Service Delivery Models	Provider
IaaS	Amazon VM Elastic Compute Cloud EC2, Google compute engine, Cloud Passage, HP converged cloud, Joyent, Linode navisite, Rackspace, etc…
PaaS	AWS Elastic Bean stalk, Cloud Foundry, Heroku, Google App Engine, etc…
SaaS	Microsoft Office 365, Onlive GT Nexus, Hewlett software, Salesforce.com, Exact Target & Calliding Cloud, etc….

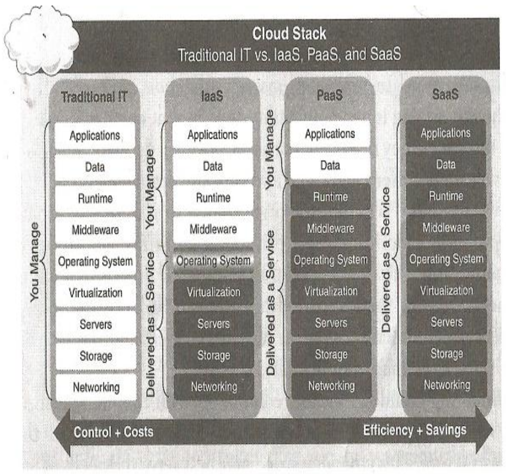

Figure1: Comparison between the traditional architecture and the cloud layers

The above diagram summarizes the three cloud offerings, who is responsible for management at each layer.

In traditional IT we have to manage all the underlying architecture which increases the control & cost. From the above figure it is clear that the control and cost increases in traditional where as efficiency and savings increases in cloud models.

As per the NIST cloud environment fall into one of the below four different models.

- Public cloud: An organization selling cloud service makes the cloud infrastructure available to large industry group or for general public. This model provides massive global scale resource – intensive capabilities such as context delivery network and cost saving through economies of scale.
- Private Cloud: whether the organization or the third party manages it on or off premises, private cloud infrastructure serves one organization. This is model of choice for IT industry which concerns more about data security and information privacy.
- Community Cloud: A specific community with common business models, security requirements (or) compliance consideration shares the cloud infrastructure. The emerging space may best serve the needs of regulated industries such as financial and pharmaceutical companies.
- Hybrid Cloud: Two or more clouds (public, private or community) makeup a hybrid cloud.

III. Advantages & Drawbacks

Advantages:

- ➔ Eliminates the need for companies to host their servers and purchase expensive software.
- ➔ Major cost savings for large business that manage and store large amounts of data.
- ➔ Reduces need for users to plan far in advance for expansion and loss of data.
- ➔ Removes need for more and expensive hardware such as memory.
- ➔ Allow users to access data across broad network on needy basis.

Drawbacks:

Cloud is being organized by human being's. Thus errors are obvious. The major drawback of cloud computing is Security and Privacy. Other are availability and possibility of data lock in, cost and time taken to transfer data on to the cloud and the risk of bugs and removing errors in large scale distributed system.

System may slow down while accessing the data due to lack of proper bandwidth.

IV. Security and Privacy Issues

Security and privacy is the important factor of concern in the cloud. Cloud is acting like a big black box, where we do not know what is happening inside the cloud. The main reason is that we are not having the control over the cloud. It is someone else securing our data. All we do is that we go on thinking that the vendor is honest and keeps our data safe. But we do not actually know how far does our assumption is true. If you see the SaaS part in the figure 1 we observe the complete control is taken by the vendor. The security issues arise due to lack of knowledge about the following for the cloud users.

1. Location: Users of the cloud do not know where their data has been stored.
2. Data Segregation: How the data of one user is been separated from the multi tenants in the cloud. Data segregation is very much important among the multi tenants of the cloud
3. Recoverability: The time taken to recover the data if something happened to the storage area. (The number of replicas presents to prevent loss and time taken to access those replicas).
4. Long Term Viability: If the company had been taken by the another what about the services it is providing to the existing customers of the company

The user without knowing all the above mentioned details just with **believing** the cloud provider or vendor proceed storing their data on the cloud.

Some vendors such as Google share the information from and to, to YouTube, Gmail (Signing into YouTube with Gmail etc…)using Application Program Interface (API) which are also called as Knowledge Program Interface (KPI) by the IT sector. This may affect the principles of data security on the cloud leading to free flow of data.

The following is a bar graph that shows about the organizations fear that avoiding them in going to the cloud storage.

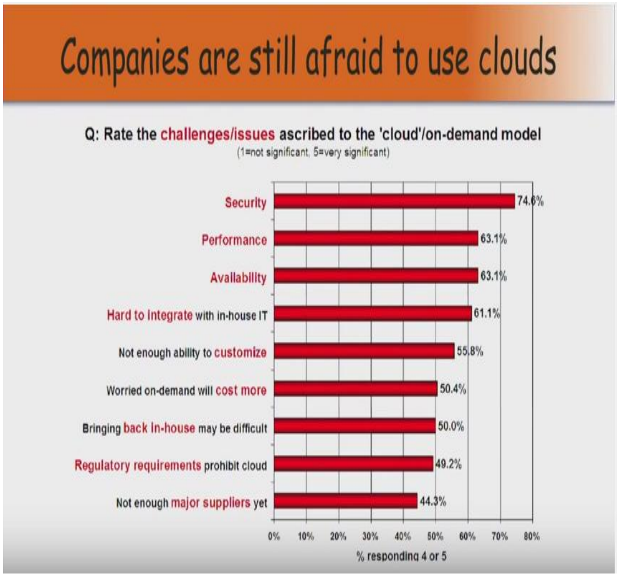

Figure 2: Survey Report

From the above graph it is clear that the three fourths are worrying about the data security. Data Security means ensuring confidentiality to our data.

They are unable to let their most confidential data on others (Vendors). Some of the other reasons are that Performance, Availability, Hard to integrate etc…

Let us observe the reason Bringing back in-house which was said by 50%. In order to understand it clearly let us take an example of non- IT industry that is a bank. If bank is storing their data on a cloud and if for suppose something happens to the data it is very difficult to manage, that too from the scratch level. This kind of problem exists in 3rd party management where loss of control, multi tenancy are the roots of the problem. Let us take an example to demonstrate this kind of fear. It had happened in the western countries. In the year 1993 the government of western countries had given a clipper chip for encryption that had been designed by National Security Agency[NSA], United States. They started mal functioning from the year 1994. In the year 1996 it had stopped working. The banks and other agencies using it were unable to recover the lost information and suffered a lot. Similarly if some vulnerable action goes on the cloud the recoverability becomes the severe threat. Though there is much fear the organization goes on to cloud assuming cloud vendor to be honest. Throughout this paper we are using the word "Trust". Trust is a relation between two entities. Generally in mathematics we have relation between entities There is no such mathematical relation that holds good for the trust. It does not satisfy mathematical relation such as symmetric which mean a=b=>b=a (In our context we may correlate as "If you trust someone they need not to trust you"), reflexive property etc… We could just give the same old ironical definition or meaning for the trust.

V. Summary

Cloud technology plays a vital role in storage of data reducing efforts in maintaining underlying architecture. As any technology has risks, cloud is also having some threats and risks. The key thing that a user should have while going to the cloud is the "Trust" on the vendor. Thus Trust is at most important factor on going to the cloud. Loss incurred if something goes vulnerable in the cloud is much greater than the profit incurred by shifting to cloud without bothering about the underlying architecture.

REFERENCES:

1) Raj Kumar Buyya, James Broberg and Andrzej Goscinski, Cloud Computing: Principles and Paradigms, ISBN- 13: 978-0470887998, Wiley press, New York, USA, February 2011.
2) To the Cloud Cloud Powering an Enterprise by Pankaj Arora, Raj Biyani and Salil Dave – TATA McGRAW-HILL EDITION.