Identification and Analysis of Risks for Cloud Computing in IAAS, PAAS and SAAS

Prof. Chitra Baggar *, Prof. Richa Sinha#

*,#Information Technology Department, Kalol Institute of Technology and Research Center, Kalol, Gujarat

Abstract— Now a days, cloud computing has been an emerging concept in the IT industry. Cloud computing is not a new technology but is a new way of using or delivering the resources. It also enhances the efficiency of computation by providing the facility of centralized database, memory processing and on demand network access.

This paper examines the different categories of risks which can be controlled or quantified. It also focuses on the analysis of risk and somewhat how to assess the risk in the cloud computing.

Keywords— *Cloud Computing, Risk, Threat, Risk Identification, Risk Assesment, Legal Risk*

I. Introduction

As per the definition of **National Institute of Standards and Technology**. Cloud computing is " a model of enabling convenient, on demand network access to a shared pool of configurable computing resources that can be provisioned rapidly and released with minimal management effort or service provider interaction."[1]

From the above definition we can say that cloud computing promises us the cost efficiency by reducing the cost of maintenance, scalability and fast service. But in fact it also introduces many risks while providing these services. The main cause of introducing risks is its multi tenancy approach and the governing policies for that multi tenant.

This paper also focuses on defining a risk management framework for clouds computing after the assessment of the risk in a cloud.

A. Cloud Computing

The cloud came into existence to model service and not he product [2]. These services may include computation, software, data access, storage and many more. The services are made available to user regardless of user unaware of the actual location and configuration of the server which is providing the services. On - demand computing and pay- as –you go model with the help of virtualization are building blocks of cloud computing [3].

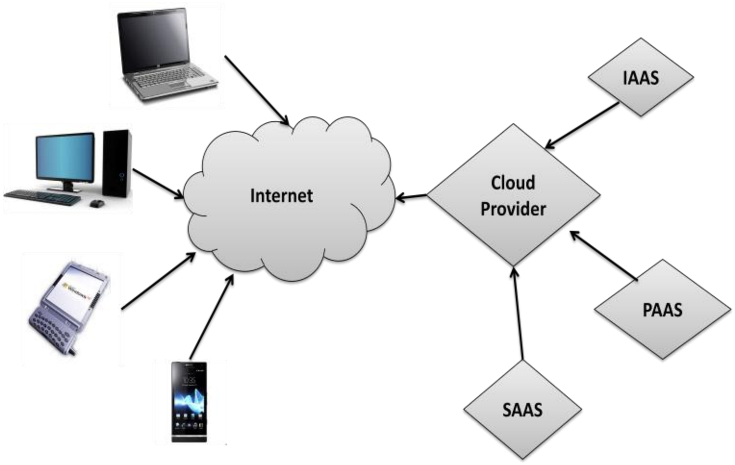


Figure 1: Cloud Architecture

As shown in figure 1, Cloud Model mainly 3 types of service[4,2]

a. Infrastructure As a Service: Providing working environment as per user wish and demand

b. Software As a Service: Providing software like storage, sharing, office and other software tools.

c. Platform As a Service: Provides infrastructure where you can create new applications

Cloud mainly consists of three types of actors. They are Service provider, one who provides only service to its end user, cloud provider, one who provides cloud infrastructure and service user, one who uses the service. Accordingly, cloud has also divided itself in three deployment model, in order to provide service to its end users. They are [2]

a. Private Cloud: Where the cloud provide and service provider lies in the same infrastructure

b. Public cloud: Where the cloud provide may differ to one who is providing service

c. Hybrid Cloud: Hybrid consists of but public and private cloud.

The main advantage of using cloud as a service is that, it reduced the end-user cost of buying resource like software and other applications.

B. Risk and Threats

The terms Threat and Risk are often used interchangeably while both are different. To control them the users of the Cloud must be aware about their differences. The term threat defines the adverse scenario applicable to a broad environment while Risk measures the probability and the impact of the given threat on the individual body or an organization. PM-BOK defines Risk[5] as 'an uncertain event or condition that, if it occurs, has a positive or negative effect on a project's objectives'.
The main characteristics of a Risk are:

1. It relates to the future.
2. It involves causes and impact.

C. Risk Planning

To control the risk in the cloud environment we have to first identify the risk and then categorize those risks into Acceptable and Non Acceptable categories. Knowing what threats are out there is an important first step in differentiating acceptable risks from those that require mitigation. After categorizing Risk as foresaid we have to plan to manage the risk. The general format[6] for dealing with Risk includes

Step 1: Risk Identification
Step 2: Risk Analysis
Step 3: Risk Prioritization
Step 4: Risk Planning
Step 5: Risk monitoring

II. MANAGING RISK IN CLOUD

To make the users of cloud environment aware about the risk in cloud computing the study of Risk in Cloud [7] is imperative. As cloud computing refers to the different service levels as SaaS, PaaS, IaaS [8,9] so the Risk will be different for each level. So before working on the Risk management first we must identify and categorize the Risk as per these services.

A. Risk in SAAS

SaaS is defined as "hosting the software and managing the deployment of infrastructure by the third party." Risks in a SaaS[10] application can be:

a. Unauthorized access of data:

Since the service provider of SaaS is also providing services to the other clients and the data of those clients are also stored at the same storage area so it is subjected to unauthorized access.

b. Incomplete and insecure data deletion:

When a customer requests his service provider to delete the data or the shared resource then it is very much possible that it will not delete the data truly and wholly due to the multi tenancy approach of cloud computing and reuse of hardware resources.

c. Data back-up or Data Replication:

Another Risk can be associated with Data back-up or replication. If any disaster occurs then whether the service provider is using sufficient amount of precautions like storing data off-site in a secure storage facility or replicate the data in any other secondary memory.

d. Lack of Standards:

The service provider must follow the standards or must be a certified service provider like SSAE16 certification.

e. Lack of Isolation:

Since cloud computing has important characteristics of multi tenancy, so there must be some distinction between all the resources (storage, hardware, memory, routing etc) of all the tenants.

f. Market Reputation of Service Provider:

If any risk affects the service provider image or reputation of service provider or failure of his business then it will be hard to the client to compensate for this

Beside these, there can be many more risks in a SaaS application

B. Risk In IAAS

IaaS is defined as '; running multiple virtual machines on a single hardware". Risks on IaaS services can be broadly categories as:

a. Business Risk due to Disaster:

If the critical application for business is hosted in IAAS environment, the down time due to man mad or natural disaster can introduce business risk.

b. Physical security of the IAAS environment[11]:

To assess physical security and environmental controls, change management, problem management, computer operations and logical security.

c. The Service Level Agreement(SLA):

SLAs are agreement between cloud user and provider. Violating SLA will also be subject to many business risks.

d. *Compatibility of IAAS and internal infrastructure*:

IAAS provider is also responsible for the virtual environment compatibility from Client to server.

C. Risk in PAAS

PaaS(Platform as a Service) provides an on demand platform where a host receives its operating system and applications from a server. Risk in PaaS[12] is broadly categories as:

a. Data Protection :

As SaaS , PaaS also have risk related to data protection as in PaaS because in PaaS also Data is stored and processed by the third party.

b. Expertise of the Service provider:

Before contacting any service provider, the client must be sure about the service providers' development team whether they have the expertise to build applications with strong information security foundation.

c. Data Location :

In cloud computing since data is stored at the third party end so the client is unaware about how the data is stored and where it is stored? Here, the question of "Where " is critical.

d. Loss of Governance:

In using cloud infrastructure, the client grants control to the Service Provider on different issues which may affect the security. While SLAs, may not offer commitment to provide such services on the part of the service provider, thus leaving a gap in the security.

e. Lack of performance due to dependency:

When the data can only be accessed via someone else's server it demands the guarantees of its uptime. The best possible uptime for an online service is almost 100% even then it is almost half a day of downtime per year.

D. Legal Risk

While a service provider supplies a cloud computing product to the customer, they draft a contract which is one sided (Service provider oriented) and most of the clauses are not clear enough that an ordinary man can understand them. Sometimes Service provider makes some changes to the agreement without giving prior information to the consumer that also led some legal issues. For example : GHOST sent an email to its consumer on 2 March 2010 that due to the changes in market place mean they were going to stop their free services and would focus on licensing services. So all the users were advised to migrate their important data to another secure place. So all of sudden these type of changes led to the legal issues and trouble to the consumers.

Another important legal risk for cloud computing may be caused by the different location of data centers, as the legal disputes handled as per the location of these data centers and the registered offices. For example ,as per the references[13] Google has patented a "water based Data Center", which is a floating platform mounted data center comprising a plurality of computing units, a sea based electrical generator in electrical connection and one or more sea water cooling units. So while identifying all the legal issues in respect of outsourcing and offshore data processing , we must also think about the maritime law.

Beside it, while considering legal issues, we must also consider a question that " Whose law we will apply, if we will have cloud dispute"? Whether we will apply U.S. law, EU Law, The customer's local law or what?

As concluded from the references [14] and before mentioned theory, we categorize the risk for all models in a general as:

a. Abuse & Malicious use of data
b. Malicious Insiders
c. Shared technology issues
d. Data Loss
e. Natural Disaster

III. ASSESMENT OF RISK USING GENERAL FORM

While identifying the risk the most common problem is the endless list of potential risks. So we must distinguish the catastrophic and likely risks. We can do it by calculating the term Risk Exposure[15]. From the

RE(Risk Exposure)=(potential damage) X (probability of occurrence) (1)

Now to calculate RE , we are using some default values assigned by the DoD(Defense of Department) and Risk Radar
Standalone(RRS) set up. These values are specified in the
following table:

Table 1: Default Assigned factors to assess the Risk

Probability (Likelihood)		**Impact (Consequence)**	
Y Axis	**Assigned Factor**	**X Axis**	**Assigned Factor**
E	.9	5	5
D	.7	4	4
C	.5	3	3
B	.3	2	2
A	.1	1	1

Table 1 detail the default values of graph as in Risk Radar[16] for Probability i.e likelihood for the risk to occur vs the impact i.e. consequences of the that assigned risk.

Table 2: Default Probability Map

Probability	**Criteria**	**Percentage**
E	Nearly Certain	90%
D	Highly Likely	70%
C	Likely	50%
B	Unlikely	30%
A	Remote	10%

Table 2 details default risk criteria from Risk Radar of probability of the risk on the base of its %.

Now using the data from the references and by using the RE formula, we are having following Risk Exposure Assessment as shown in Table 3:

Table 3: The derived risk exposure after experimentation

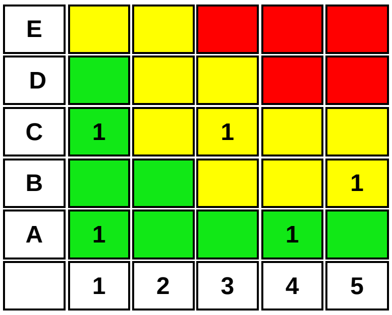
Reference	**Risk**	**Likelihood**	**Impact**	**Risk**
R1	Abuse & Malicious use of data	0.5	1	0.5
R2	Malicious Insiders	0.5	3	1.5
R3	Shared technolog	0.1	4	0.4

	y issues			
R4	Data Loss	0.3	5	1.5
R5	Natural Disaster	0.1	1	0.1

The default Risk Level Ranges are as following:

Low	: 0.1 through 0.7
Medium	: 0.8 through 2.5
High	: 2.6 through 4.5

As shown in the table 3, we found out following Probability Impact matrix as shown in Figure 2.



E	🟨	🟨	🟥	🟥	🟥
D	🟩	🟨	🟨	🟥	🟥
C	🟩 1	🟨	🟨 1	🟨	🟨
B	🟩	🟩	🟨	🟨	🟨 1
A	🟩 1	🟩	🟩	🟩 1	🟩
	1	2	3	4	5

Figure 2: Probability Impact factor of risk as classified

In above figure, **Green** color grid shows the Risks which are having Low Exposure, **Yellow** is for Medium and **Red** for High Risks.

IV. Conclusion

To fulfill the expected outcome as promised by the technology, Cloud computing must offer high information security . As cloud computing is an emerging field and the users of the technology is growing day by day, so the users must be aware about the different issues and risks involved in using the technology. The user and the service provider must distinguish the most likely and severe risks so that the necessary risk control methods can be developed accordingly.

From this study, it can be concluded that still there is a lack of risk identification approach and risk control techniques for Cloud computing. So we think that the introduction of new risk analysis approach has significant importance and scope.

References

[1] P. Mell and T. Grance,"The NIST Definition of Cloud Computing",defination of Cloud computing given by National Institute of Standards and Technology, Information Technology Laboratory,Jul-2009

[2] Wikepedia, "Cloud computing", Reference Link http://en.wikipedia.org/wiki/Cloud_computing.

[3] R. Sinha, N. Purohit , H. diwanji,"Energy Efficient Dynamic Integration of Thresholds for Migration at Cloud Data Centers",Int. Journal Of Computer Application, Dec 2011

[4] Diversity Limited, Rackspace Hosting, "Understanding The Cloud Computing Stack SaaS, Paas, IaaS", 2011

[5] C. S. Snyder, Book on "A User Manual to the PM BOK Guide", Wiley Copyright 2010

[6] Department of Defense,Risk Managment Guide for DOD Acquisition 6th Edition (Version 1.0), Aug 2006

[7] European Network and Information security Agency(Enisa)," Cloud computing: benefits, risks and recommendations for information security"2013

[8] Carnegie Mellon University CERT, "Cloud Security: Evaluating Risks within IAAS/PAAS/SAAS" Manual by Tech Target Organization, May 2012

[9] Cloud Security Alliance,"Top Threats to Cloud Computing V1.0", Manual ,Mar 2010

[10] InterisTM, "Software – as – A- service,Cloud Service , Risk assessment", Manual ,2013.

[11] A Technologies and SearchCloudSecurity.com, E guide on "Evaluating IaaS security risks" Jul 2011

[12] The Open Web Application Security Project (OWASP)," Cloud - Top 5 Risks with PAAS" , Referenced by <https://www.owasp.org/index.php? title=Cloud_-_Top_5_Risks_with_PAAS&setlang=es>

[13] Queen Mary, university of London,"QMUL Cloud Legal Project" Reference Link http://www.cloudlegal.ccls.qmul.ac.uk/

[14] C. Lim, A. Suparman "Risk Analysis and Comparative Study of the Different Cloud Computing Providers in Indonesia" , Cloud Computing and Social Networking (ICCCSN), IEEE, Oct 2012.

[15] B. Hughes, M. Cotterell,R. Mall, Book on "Software Project Management", 5th Edition,Chapter No.7.

[16] 13Pro - concept, LLC," Risk Radar 2012 User Guide",2012