International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

An Identification of Framework for Secure Cloud Computing

Dipti Singh Galav[1], S. M. Ghosh[2]

[1]Chhattisgarh Swami Vivekanand University, Rungta College of Engineering and Technology, Bhilai, Chhattisgarh, India

[2]Chhattisgarh Swami Vivekanand University, Rungta College of Engineering and Technology, Bhilai, Chhattisgarh, India

Abstract: ***Today cloud computing is a way which delivers services very fast, at low cost and more productivity. It is easily accepted by people. But there is also one area which is the biggest factor which probes the peoples for using this service i.e. "Cloud Security". There are various frameworks available regarding cloud security, in this paper we have proposed framework which will take care of better security for secure cloud computing.***

Keywords: Cloud Computing, NIST, IaaS, PaaS, SaaS

1. Introduction

Cloud computing is growing technology or it is a way which provides the fastest way to deliver the services in IT industry. It is available with new features like on-demand network access, virtualization, and convenient network access, pay-as-you-go. The biggest issue in cloud computing is security and privacy because of this issue many organization does not want to move to cloud.

2. Background

There are many definitions of cloud computing but in this paper we had preferred NIST's(National Institute of Standard & Technology) definition .The NIST definition of cloud computing is (NIST 2009a):

"Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."

NIST's definition is defined by three services, five key characteristics and four deployment models they are:

2.1 Cloud Delivery Service Model

There are three types of services provided by cloud providers:

1. **Infrastructure as a service (IaaS):-** The IaaS service is the lowest service model and offers infrastructure resources as a srvice, like raw data storage, processing power and network capacity. The customer can use IaaS service to deploy operating systems and applications. In this customer does not need to manage cloud infrastructure his control is limited to only operating syestem, storage and application.
2. **Platform as a service (PaaS):-** PaaS provides operation and development of platforms. Customer does not need to manage infrastructure, they can only deploy and run their application.
3. **Software as a service (SaaS):-** It offers applications to the customer. Customer has to manage the applications, operating system and infrastructure also.

2.2 Cloud Deployment Models

There are four types of deployment models in cloud:

1. **Public cloud**
   This architecture runs publically means there is entrusted users who are not employee of any specific organization. This is totally managed by cloud service provider.
2. **Private cloud**
   This model runs within a single organization, there are trusted users. There is a contractual agreement between organization and cloud service provider.
3. **Community cloud**
   This model runs by a community within a single organization, there are trusted users. It is simply like private cloud.
4. **Hybrid cloud**
   This model is combination of public, private and hybrid model. There are both types of users, trusted and entrusted. Entrusted users are prevented to access the private and community services.

2.3 Characteristics of Cloud Computing

There are some features of cloud computing is explained:

1. **On-demand network access**
   Cloud computing resources can be procured and disposed by the consumer without interaction with the cloud service provider.
2. **Resource pooling**
   It enables the sharing of virtual and physical resources by multiple users, "dynamically assigning and releasing resources according to consumer demand"(NIST 2009a).
3. **Broad network access**
   Cloud services are accessible over the network via standardized interfaces, enabling access to services not only

by complex devices but also by light weight devices like smart phones.

4. **Rapid elasticity**
   Cloud capabilities can be easily increased if the demand rises, and releasing the capabilities when the need for drops.
5. **Measured services**
   Cloud computing enables the measuring of used resources, it provide the "pay-per-use" model.

3. Related Studies

National institute of standard & technology (2013), provides security control for federal information system.

Ahmed E.Youssef, Manal Alageel (2012), propose a Framework for secure cloud computing. They identified Security and privacy requirements, attacks, threat and Risk associated to deployment model.

National institute of standard & technology (2011), Definition of cloud computing. It provides standard definition of cloud computing, it defines essential characteristic, service delivery model, cloud deployment models.

National institute of standard & technology (2010), It guides how to apply Risk Management Framework in federal information system. It integrates information security and risk management process with system development life cycle.

Capgemini (2010), publish a white paper on "Cloud Computing & Confidentiality". It defines a framework with respect to confidentiality. When putting the technical security control in cloud environment they found some limitation like access limitation, security assuration and physical separation limitation

Brodkin(2008) discussed cloud security which points out seven areas of security issues in cloud computing :

- **Privileged user access:**
  Data stored and processed outside the enterprises direct control. Brodkin advises to get as much information as possible about the people who manage your data and the controls they implement.
- **Regulatory Compliance:**
  Cloud computing provides who refuse to undergo this security are signaling that customers can only use them for the most trivial functions.
- **Data Location**
  The exact location of the data in the cloud is unknown. Data may be located in systems in other countries, which may conflict with regulations. Gartner advises to investigate if cloud providers will commit to keeping data in specific jurisdictions and whether the providers will make contractual commitments to obey local privacy requirements on behalf of their customers.

1. **Data Segregation**
   Encryption is used to segregate the data. It is advised to do through a evaluation of encryption systems used by the cloud providers.
2. **Recovery**
   Cloud providers should have recovery mechanism in case of disaster. "Any offering that does not replicate the data and application infrastructure across multiple sites is a vulnerable to a failure".
3. **Investigative Support**
   Gartner warns that "investigating inappropriate or illegal activity may be impossible in cloud, because data and logging may be co-located and spread across ever changing sets of hosts and data centers". Cloud providers cannot provide customers with contractual statement specifying support for incorruptible logging and investigation.
4. **Data Lock-in**
   Availability of customers' data may be at risk if a cloud provider goes broke or is acquired by another organization. Providers should provide procedures how customers can retrieve their data when needed and in which format data is presented in a format proprietary to the cloud provider.

National institute of standard & technology (2008), provides a guide for mapping types of information and information system to security category. It recommends security categorization process describe a methodology for identifying type of information and information system, suggest provisional impact level.

4. Related Framework

The framework which is defined by capgemini(2010).

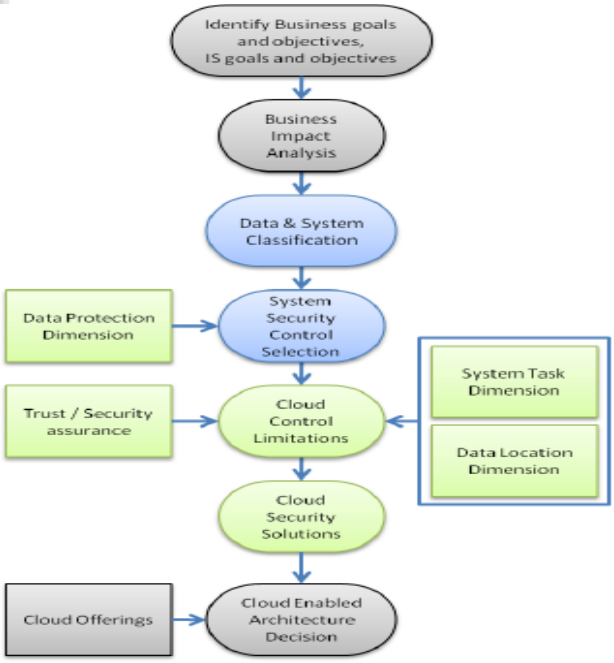

Figure 1: Cloud computing confidentiality framework

In this framework, capgemini uses technical security control, focuses on data confidentiality, data location dimension. When applying technical security control they found some limitation like baseline control limitation, optional control limitation, security assurance limited, access related limitation. Finally it results:

1. Classified data
2. Security with respect to architecture
3. Cloud security solution- 1) Don't enter in cloud 2) Use hybrid cloud 3) Provide control of public cloud in both side i.e. cloud provider, customer.

5. Proposed Framework

With the study of available framework and identifying its strength and weaknesses, we have proposed a framework which will address the problems not addressed in the previous framework. In previous framework there is some Laguna that we have identified these are as follows:-

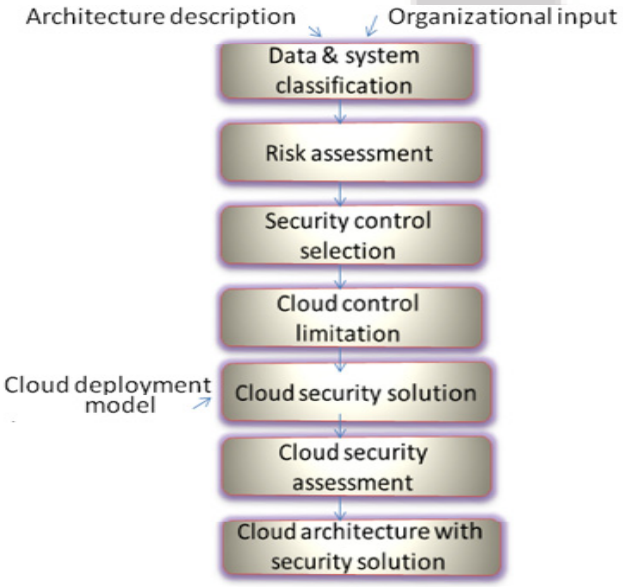

Figure 2: Proposed framework

1. Cloud risk assessment: In previous framework it did not explain about cloud risks. It is very important phase after classifying the data and reduces work overhead, that's why we have added this phase in my proposed framework.
2. Cloud security assessment: This is the important phase for cloud secure framework, because after giving security solution it is necessary to assess the security solution so that we can decide what level of information assurance the data requires i.e. Confidentiality, integrity and availability. It should be cleary written in agreement.

6. Working of Proposed Framework

Input: Architecture description, organization's mission, objective, goal.

Step1. Data and system classification

a) Identify type of information:- There are three types of information
- Management information
- Service delivery support information
- Administrative information

Figure 3: Type of information

Government Resource Management Information			
Administrative management	Human resource management	Information and Technology Management	Supply chain management
Security management, help desk service, travel, fleet and equipment management	HR strategy, Staff acquisition, employee relation, labor relation	Lifecycle change management, System maintenance etc.	Goods acquisition, service acquisition, inventory control etc.

b) Security categorization of information with respect to confidentiality, integrity and availability.

Figure 4: Security categorization of information

Information type	*Confidentiality*	*Integrity*	*Availability*
Control and oversight			
Corrective action, Program monitoring, Program evaluation	low	low	low
Regulatory Development			
Rule publication, regulatory development	low	low	low

Step2. Risk Assessment

It includes processes:
- Risk identification:- It is the process of finding, recognizing and recording the risk,
- Risk analysis: - It involves causes and sources of risk.
- Risk evaluation: -It helps to take decision like whether a risk needs to be treated, what are the priorities for the treatment, which number of path should be followed.

Cloud Risk Factors:
- Data security: - Because business data resides in provider side, so there are chances of theft, hacking of data.
- Service reliability: - Loss of internet connectivity.
- Software management:- Without control over the software edits and updates of software are very complex.

Step3. Security control selection

There are three types of security controls:
a) Technical
b) Management
c) Operational

Security control classes, families and identifiers:

National institute of standard and technology (NIST) defines seventeenth classes of security controls, but I am showing here only two identifiers:-

Figure 5: Security control classes, families and identifiers

Identifier	*Family*	*Class*
CA	Security assessment and authorization	Management
RA	Risk management	Management

Process of security control selection

Select baseline control

I will select baseline control from the below table which is given by National Institute of Standard and Technology (NIST).

Figure 5: Selection of initial baseline control

Control no	*Control name*	*Priority*	*Initial control baseline*		
			Low	Moderate	High
Security assessment and authorization					
CA-1	Security assessment and authorization procedure and policies	P1			
CA-2	Security assessment	P2			
CA-3	Information connection	P1			
CA-4	Security certification	P3			
CA-5	Plan of action	P3			
CA-6	Security authorization	P3			
CA-7	Continuous monitoring	P3			
Risk assessment					
RA-1	Risk assessment policy and procedure	P1			
RA-2	Security categorization	P1			
RA-3	Risk assessment	P1			
RA-4	Risk assessment update	P1			
RA-5	Vulnerability scanning	P1			

- **Tailoring the baseline control**
  Tailoring the baseline control by applying scoping, parameterization, and control guidance.
- **Supplementing the baseline control**
  If baseline control is not sufficient for achieving the required protection then add other controls.

Step 4. Cloud control limitation

- **Baseline control limitation**
  Check whether baseline control fulfills the requirement or not, if not take some optional control to achieve the goal.
- **Optional control limitation**
  Check what the limitations after applying optional controls are.
- **Access related limitation**
  If cloud service is accessed by external network and no encryption is supported then cloud computing is limited to lowand public access system.
- **Security assurance limitation**
  In cloud there is no assurance is given to customer by provider for security.
- **System separation limitation**
  Physical system separation is limited because in cloud it uses virtualization concept which makes cloud effective, if system separation system is done then it will be a traditional internet system.

Step 5. Cloud security solution

It may be which cloud deployment models like public, private, hybrid is used. The solution may be some part of public cloud should be under control of recipient also.

Step 6. Cloud security assessment

It depends on some factors like:

- **Identify what type of cloud based service:-** Identify which deployment models and service delivery is suited to organization.
- **Identify who is data controller:-** It should be written in service level agreement where data is located.
- **Decide what level of assurance data requires:** Means that confidentiality, integrity, availability should be written in service level agreement.
- **Confidentiality**: - How much protection is given to data when transit and storage, it always need to be encrypted.
- **Integrity: -** More confident data will not be interfered.
- **Availability: -** Provide instant access always.

Step7. Cloud architecture with solution

Finally we get cloud security solution with enabled architecture.

.

References

[1] *Blank M*. et. Al. 2011, NIST Definition of Cloud Computing, published by National Institute of Standard and Technology.
[2] *Evans D*. et. Al. 2004, Standard Security Categorization for Federal Information and Information System.
[3] *Goyal* B. et. Al. 2012. Reminiscing Cloud Computing Technology,IJRET
[4] http://en.wikipedia.org/wiki/Cloud_computing
[5] *ISO/IEC* Guide 73:2009 (2009). *Risk management — Vocabulary*. International Organization for Standardization
[6] *Locke* G., Gallagher. P. 2010. Guide for applying the Risk Management Framework to Federal information systems NIST's special publication800-37
[7] *Locke G.* et. Al. 2009, Recommended Security Control for Security of Federal Information System and Organization. published by National Institute of Standard and Technology.
[8] *Pieters* Ir., Hartel P.2010, Cloud Computing and Confidentiality Capegemini
[9] *Rebcca M. Blank* 2013, Security and Privacy Control for Federal Information System and Organization, published by National Institute of Standard and Technology.
[10] *Stine K*. et. Al. 2008, Guide for Mapping Types of Information and Information System to Security Category, by National Institute of Standard and Technology

Author Profile

Dipti Singh Galav received the B.C.A. degree from Pt. Ravishankar Shukla University in 2007 and M.C.A. degree from Chhattisgarh Swami Vivekanand Technical University in 2010. Recently have registered as Ph.d. scholar in Chhattisgarh Swami Vivekanand Technical University.