www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume – 5 Issue -02 February, 2016 Page No. 15856-15858

A Review On Security Issues In Cloud Computing

Mr.Vishesh P.Gaikwad(Asst. Prof)
Computer Science and engineering Department
Priyadarshini Bhagwati college of Engineering, Nagpur University

***Abstract*— The data security in cloud is an important issue. The important data can be stored in cloud and the security of that data is totally dependent on cloud. The data might be uncovered by the malicious third party user because of wireless connection between client and cloud without proper authentication and protection. In this paper we figure out the different security issues with the cloud . When the data is stored in cloud the data should be properly managed and cloud have to provide a proper security to the data. In this paper discussing the different type of issues with the cloud and also possible policies are mentioned here that we can take care of those issues while discussing about the security provided by the cloud.**

***Keywords*- Cloud storage, Security in cloud.**

Cloud computing [1] is the use of computing resources that are delivered as a service over a network The name comes from the use of a cloud-shaped symbol as an abstraction for the complex infrastructure it contains in system diagrams.. It is cost effective development of a scalable web portals on highly available and fail safe infrastructure. The evolution of cloud can handle a massive data as per on demand service so this is a cost effective technique to store data on cloud.

Cloud [5] computing can be seen as a service-oriented architecture (SOA) explore every computing environment for providing security trust issues. Facing cloud computing, a prerequisite control measure is to ensure that a concrete Cloud computing Service Level Agreement (SLA) is put in place and maintained when dealing with outsourced cloud service providers and specialized cloud vendors. Due to the nature and demand of emerging cloud technologies, there is a certain degree of inexperience when dealing with cloud security. Currently Cloud computing clients have to trust 3rd party cloud providers on many fronts, especially on the availability of cloud service as well as data security. Therefore the SLA forms an integral part of a client's first line of defense. The SLA thus becomes the solitary legal agreement between the service provider and client.

I. TYPES OF CLOUD

For providing a secure cloud computing solution [5], we have to decide which type of cloud are to be implemented .Mainly three types of cloud modes which are public, private and hybrid.

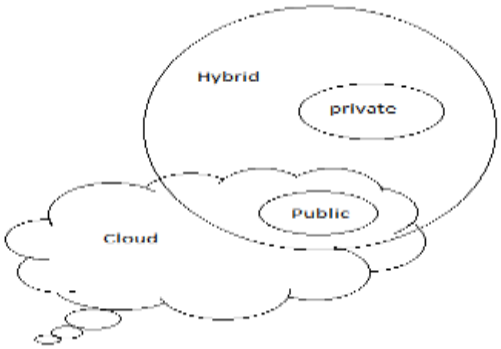

Figure 1: Cloud Computing Types

As shown in figure 1 the different types of cloud and are explained below.

A. Public Cloud:

A public cloud is a model which allows users' access to the cloud via web browsers. It is based on a pay-per-use model, It is similar to prepaid balance of mobile you can make a call if the prepaid balance is available if your balance is finished then you are not able to make a call. Cloud clients are happy pay per use manner and now this cloud is used widely in the IT infrastructure [9]. This type of cloud is less secured than the other types of cloud. Therefore trust and privacy concerns are rife when dealing with Public clouds with the Cloud SLA at its core. A key management consideration, which needs to be answered within the SLA deals with ensuring that ample security controls are put in place. One option is for both the cloud vendor and client mutually agree in sharing joint responsibility in enforcing cloud checks and validation are performed across their own systems.

B. Private Cloud

A private cloud [5] is set up within an organization's internal enterprise datacenter. It is easier to align with security, compliance, and regulatory requirements, and provides more enterprise control over deployment and use. In the private cloud, scalable resources and virtual applications provided by the cloud vendor are pooled together and available for cloud users to share and use. It differs from the public cloud in that

all the cloud resources and applications are managed by the organization itself, similar to Intranet functionality. Utilization on the private cloud can be much more secure than that of the public cloud because of its specified internal exposure. Only the organization and designated stakeholders may have access to operate on a specific Private cloud.

C. Hybrid Cloud

Hybrid cloud [5] is a combination of two or more cloud. The other clouds are bound together offering the benefits of others into one hybrid cloud. It provides a lack of flexibility, security for in-house application. It provides flexibility in in-house application with fault tolerance and therefore it is not scalable.

II. SECURITY BETWEEN CLOUD CLIENT AND CLOUD SERVICE PROVIDER

Knowing that there are possibilities for security and trust issues on both sides of the cloud customer-provider relationship allows us to separate what each side should do to build a secure system. This is a paradigm shift from a traditional model where software and computing resources were both provided in-house. While in the internal model, system and network security was mostly handled by the system and network engineers, so even an insecure piece of software would only be accessible to people within the company and particularly [12]

Layers and Obligations for Cloud Security:

In the cloud model [9], the network engineers are not concerned with these problems and it is up to the cloud customer to protect their data.

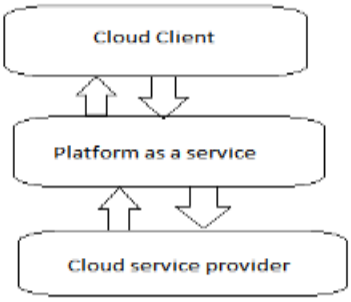

Figure 2: Example of the separation of security concerns between a PaaS customer and provider.

Note that there is some overlap where the two meet Take Figure 2 as an example. Here the provider is providing the platform as a service to the customer. The customer is responsible for writing software that runs on top of the platform and for ensuring the security of data up to the point it is given to the platform service. This should include encrypting the data if the cloud provider does not do a satisfactory job of protecting the data (i.e. using a weak cipher, the details of which *should* be disclosed when signing up for the service). The provider is responsible for securing the infrastructure (network connectivity, physical machines, and platform environment). When the underlying provider services meet the customer software implementation there should be a clear, well defined interface for transferring data

II. RELATED WORKS

SECURITY ISSUES & POLICIES IN CLOUD COMPUTING

Cloud computing is a new computing model, this model have a different cloud computing issues:

A. ***Security issue in cloud computing***

a) In Cloud computing boundaries are not defined clearly for protecting the device user, the traditional computing model can protected device user by dividing physical and logical security zones.

b) Service security issues. [6]
The service provider controlled the data and other resources. If the providers not providing proper security to data stored in cloud .Then the confidentiality of data should be reduce.

c) Protection for user data:[1]this issue is about to protecting data storage, data recovery, data integrity data encryption and the address of the user.

d) The number of user's changes dynamically, as well as user uses the different services, leading the user can not be classified.

e) The cloud service provider[3]has more rights than the user, therefore we have to manage the balance between the service provider and service provider becomes a problem

f) Cloud computing [11] have a complex structure and user can dynamically changes in the cloud environment, thus the security and integrity is an important issue to be considered.

g) A multi-tenancy trusted computing environment model (MTCEM)[2] is designed for IaaS delivery model, main aim is to assure a trusted infrastructure to a client .it provide a two level hierarchy chain to provide a cloud customers control and provide computing platform in cloud. Its also provide a mechanism that provide assure the IaaS platform by cloud service provider is trusted.

h) There are two main approaches. First approach is the main focus on the gap that is slowing down the cloud adaption and reviewing the threat challenges. And second approach is discussing about to address some of the widely attacks using machine learning techniques. Cloud server and the customer's tool that protect themselves from known or unknown security issues

B. Security policy in cloud computing

To solve this problem there are some important policies as we shown below.

a) We can divide cloud into multiple domains, and an each domain has a different kind of security according to domain the security is to be provided. the domain is to be divided as a global or local.

b) Check that the user's connection and communications security with the SSL, VPN, PPTP, etc. Using license and allowing and providing multiple authorizations among user, it should be ensure that the data travelled securely between a consumer and service provider.

c) User data security assurance: According to requirement the security is to be providing to a client or consumer .It must be assured that the security is important.

d) Using a series of measure to solve the user dynamic requirements, including a complete single sign-on authentication, proxy, collaborative certification, and certification between security domains.

e) Establishment of third-party monitoring mechanism to ensure that operation of cloud computing environment is safe and stable.

f) The computing requested by service requestor, should carry out the safety tests, it can check whether they contain malicious requests to undermine the security rules.

III. CONCLUSION

In this paper we are discussion different issues and also provide some of the important policies. This policies is useful for maintaining the data on the cloud .This policies is helpful to provide a provide security to the cloud data. These issues are also have to keep in mind while data are stored in the cloud and also apply the possible solutions for those issues with the cloud.

REFERENCES

[1] Rimal, B.P., Eunmi Choi and Lumb, I. "A Taxonomy and Survey of Cloud Computing Systems". *International Joint Conference on INC, IMS and IDC, Seoul*, 2009.

[2] Nuno Santos, Krishna P. Gummadi, Rodrigo Rodrigues, "Towards Trusted Cloud Computing", International Conference on *Hot topics in cloud computing*, 2009.

[3] Grossman, R.L., "The Case for Cloud Computing", *International Conference on IT Professional*, March-April, 2009.

[4] Wang Han-zhang, Huang Liu-sheng "An improved trusted cloud computing platform model based on DAA and Privacy CA scheme"-2010.

[5] Ramgovind S, Eloff MM, Smith E "The Management of Security in Cloud Computing"-2010.

[6] Xiang Tana, Bo Aib "The Issues of Cloud Computing Security in High-speed Railway"-2011

[7] Shahryar Shafique Qureshi1 , Toufeeq Ahmad1, Khalid Rafique2, Shuja-ul-islam3 "Mobile cloud computing as future for mobile applications – implementation methods and challenging issues"-2011.

[8] A Platform Computing Whitepaper, 'Enterprise Cloud Computing:Transforming IT', *Platform Computing*, pp6, viewed 13 March 2010.

[9] Vijay Varadharajan Udaya Tupakula TREASURE: Trust Enhanced Security for Cloud Environments "2012

[10] Eman M.Mohamed Sherif EI-Etriby " Randomness Testing ofModem Encryption Techniques in Cloud Environment"

[11] Yu Shyang Tan "Tracking of Data Leaving the Cloud" 2011

[12] Farhan Bashir Shaikh " Security Threats in Cloud Computing"2011