Trust Issues in Cloud Computing

Adesh kumar
SLBSRSV, New Delhi, India

Abstract- Cloud computing is the computing paradigm in which computing resources are used by cloud customer on metric basic. This reduces the hardware and software cost for cloud customers. The cloud customer has the flexibility to variably choose cloud resources and pay only on basic of their utilization. There are many factors which affect cloud customers to decide whether the cloud should be used or no. The main two factors are trust and security which always create doubt in new cloud users. In this paper I will discuss about the trust which is an important and integral part of cloud computing. The trust is the one of main factors which makes a cloud successful.

Keywords- Cloud computing, trust, security

I. INTRODUCTION

In cloud computing computer resources such as computer hardware, software, networks, database and computing time are provided on pay per use basis to the cloud users. In cloud computing the cloud user do not have direct access to cloud resources instead cloud resources are provided in form of services. Cloud computing is a technique or model in which all computer resources are made available to the user on pay per use basis. A cloud user can buy any computer resource as per his/her requirement for limited period of times. The cloud users can pay only how much resources are consumed by them and for how much time they have used them. Cloud can be deployed differently as per requirements of cloud users. The cloud deployment model can be categorized as private cloud, public cloud, community cloud and hybrid cloud. There are various services which are provided on cloud by cloud service provider such as Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), Network as a Service, Security as a Service (SaaS), Communication as a Service, etc.

A. Cloud Deployment Models-

First I discus the different types of cloud deployment models as follows:

- *Public cloud-*

  A public cloud is design in such a way that it is always available for public to meet their service demands. Anyone can buy cloud resources from this type of cloud. It differs from the public cloud in that all the cloud resources and applications are managed by the organization itself, similar to Intranet functionality. Use of services 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 a specific Private cloud.
- *Private cloud-*

  A private cloud is designed for a specific organization to meet its requirements. In private cloud only the person of that organization can use private cloud and avail services available on private cloud. Shared infrastructure, remote hosting, and dynamic licensing and provisioning are strong attraction for a company. Public cloud implementation can be a big help in removing the problem of infrastructure maintenance by IT organizations.
- *Community cloud-*

  It can be think of residing somewhere between a private cloud and a public cloud, community cloud describes a shared infrastructure that is employed by and supported by multiple companies
- *Hybrid cloud-*

  A hybrid cloud is combination of two or more clouds. The participants of this cloud may private cloud, public cloud or community cloud. It is defined by NIST as “a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability.

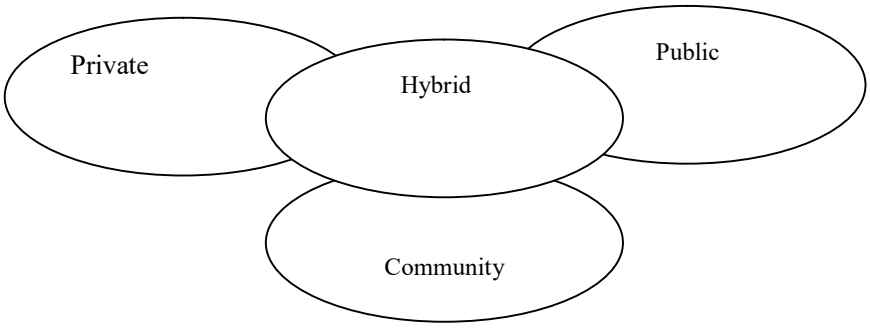

Figure 1. Cloud deployment models

B. Cloud Service Model-

- *Software as a Service (SaaS)-*
  The application software are provided to the cloud user as a service in Software as a Service (SaaS). The cloud users buy the applications or software as per their requirements through this service model. This model allows customers to use applications available on the cloud. The customers have no control over system platform and infrastructure.
- *Platform as a Service (PaaS)-*
  In these types of service model, platform is provided to cloud users so that cloud users can install and run their software on that platform. This type of model allows customers to use hosting environment including programming language, database, libraries, application tools, etc.
- *Infrastructure as a Service (IaaS)-*
  In this type of service model infrastructure is provided to the cloud users so that the cloud users can use cloud's infrastructure. The cloud infrastructure includes processing power, network, storage etc. This service allow cloud customer to run and deploy their various software on cloud infrastructure. In this model customers have full control over application and infrastructure.
- Security as a Service-
  In security as a service the security management of the organization is handled by cloud service provider. The cloud service provider is responsible to tackle all the threads and security issues of the organization which buy security as a service from cloud service provider.

II. TRUST ISSUES IN CLOUD

These are the factors which can be used to establish trust between cloud user and cloud vendors to deliver cloud services

A. Data Isolation-
The cloud uses many applications running concurrently. The application should be run in isolation to one another. There are many users that share cloud's hardware and software resource. Therefore the data of all users must be kept in isolation so that one user cannot see other's data.

B. Multi tenancy-
Public cloud has the nature of multi tenancy. Many different types of users can access cloud. Therefore it is big challenge to stop unauthorized users to access stored data and moving data in cloud

C. Availability-
Availability is the guarantee that cloud resources will be provided to cloud user when a request is made for. The cloud vendor should assure to the cloud customers that when user requests a service then that service will be provided without delay.

D. Reliability-

Reliability refers that cloud system should not fail to deliver service on demand. The data stored by cloud user should be safe and delivered to users when demanded.

E. *Confidentiality*- The information of cloud user should be kept safe and secure. Information store in database cannot be accessed by unauthorized users intentionally or unintentionally

F. *Identity management*-
Identity management is a technique by which only authorized users and access data and resources. User id and password are the simplest form of identity management. But in cloud more robust techniques are used to secure cloud data and resources.

G. *Cryptography*-
Cryptography is a technique by which data is keep secure from hackers. In cloud computing data of different users are in motion so with the help of cryptography data is coded so that unauthorized users can not access that data.

H. *Transparency*-
Transparency is one of the key features to gain trust of customer. The transparency should be kept in cloud computing with the cloud users.

I. *Maintenance*-
Maintenance is the surety that if system fails any how cloud users data will not be lost. The maintenance of cloud resources should be executed periodically.

J. *SLA definition*-
The service level agreement is an agreement between cloud user and cloud vendor. The service level agreement should be clear and easy to understand so that it can build trust cloud user trust. All parameters should be clearly mentioned in SLA. SLA is the first thing that can attract cloud user trust.

III.CONCLUSION

Cloud computing is evolving very fast and every one want to use cloud computing in one or other way. But cloud computing is new technology; therefore cloud users have some doubts in their mind about the safety and security of their data. So trust is a key factor in cloud computing. A trust should be made by cloud vendor by applying various means. I discussed some issues related to trust in this paper but issues are not limited to discuss here.

REFERENCES

[1] R. L. Krutz and R. D. Vines, "Cloud Security: A Comprehensive Guide to Secure Cloud Computing", Wiley Publishing, 2010

[2] J. W. Rittinghouse, and J. F. Ransome," Cloud Computing: Implementation, management and Security", CRC Press, 2010

[3] W. Jansen,And T. Grance, DRAFT: Guidelines on Security and Privacy in Public Cloud Computing, NIST, U.S. Department of Commerce, Special Edition 800-144,January 2011

[4] B. R. Kandukuri, et al., "Cloud Security Issues": IEEE International Conference on Services computing, 2009

[5] W. Jansen,And T. Grance, DRAFT: Guidelines on Security and Privacy in Public Cloud Computing, NIST, U.S. Department of Commerce, Special Edition 800-144,January 2011

[6] W. Juang and Y. Shue. "A Secure and Privacy Protection Digital Goods Trading Scheme in Cloud Computing", 2010

[7] G. Ling, D. Fu, J. Zhu and G. Dasmalchi, "Cloud Computing: IT as a Service", IEEE Computer Society, April 2009