SECURITY THREATS IN CLOUD COMPUTING

Neha Kajal
CSE & IT department
ITM University
Gurgaon, India
nehakajal92@gmail.com

Nikhat Ikram
CSE & IT department
ITM University
Gurgaon, India
nk24786@gmail.com

Prachi
CSE & IT department
ITM University
Gurgaon, India
prachi@itmindia.edu

***Abstract*— Computing in cloud has come out as a growing trend that has eliminated the burden of hardware and software infrastructure by facilitating virtual machines via internet. In spite of the indispensable advantages, cloud computing also brings critical challenges that cannot be avoided from consumer side if the security of the data is concerned. In this paper, we analyze the various security aspects that are vulnerable to the cloud computing and needed to be resolved. This will help to upgrade promising benefits of cloud computing so that consumers cannot have a second thought regarding its adoption.**

Keywords—security; cloud; security threats; cloud computing; data security.

I. INTRODUCTION

Computing in cloud hosts and delivers the various processed work that is send over the web servers. It is an emerging paradigm which is multiplying its importance both in business and IT sector. It enables convenient on demand network access to a shared pool of configurable computing resources on rent basis [1-5]. The services provided like storage, processing etc are operated with the help of web servers known as 'cloud 'and the GUI which is imparted by the customer's browser. This technology was introduced around 1960 and has multiplied its use since last decade. Introduction of various technologies like virtualization has evolved cloud along with various services that can be rapidly provisioned over the web with minimal efforts.

Cloud Computation provides customers the illusion of having a large computation infrastructure which is ready whenever need arises. Cloud computing offers several unique features, such as:

A. Multi Latency

IT infrastructure is shared on the rent basis as a resource, service or as a platform

B. Large Scale

In order to widespread its access in terms of storage and range, this computing system includes numerous servers and PCs.

C. Rented service delivery model

Instead of buying software and hardware, users needs to pay for the asset on temporary basis.

D. Reliability, usability and extensibility

Cloud helps in secure storage of user's data without worrying about the issues like software updation, viruses, data loss.

E. Flexibility

Services can be used anywhere, anytime. Moreover, they can be easily scaled up and down.

F. Virtualization

With the help of virtualization, all the infrastructure services can be virtualized. Therefore, users can access services with the help of web and get data from cloud on rental basis rather than maintaining their own resource pool.

Although, cloud computing offers a great opportunity for effective utilization of infrastructure and removal of workload from client yet it comes with security risks that are unavoidable. The security risks involved in cloud environment can be categorized on the basis of different components of cloud. Component of cloud are further classified in layered manner.

The highest layer (public cloud, private cloud, community cloud, hybrid cloud) represents the deployment models. The second layer represents the service models (SaaS, PaaS, IaaS) [6] that are utilized as an application service within a particular deployment model. The third and final layer depicts essential characteristics provided by the cloud.

Cloud computation faced certain security challenges regarding its storage, transmission, authentication, application

ISBN:978-1-4799-8890-7/15/$31.00 ©2015 IEEE

level security and security related to third party resources [7-10]. Challenge varies according to the selected service model.

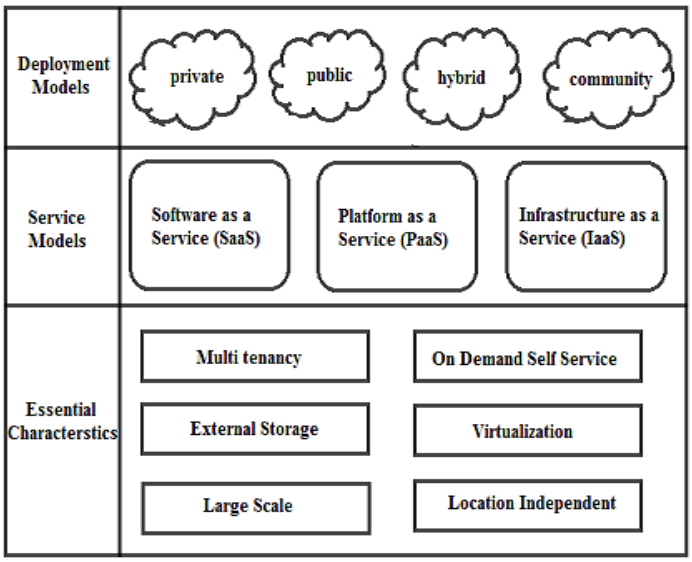

Fig. 1. Cloud Components

II. CLOUD DEPLOYMENT MODEL

In order to understand the security issues, initially we will discuss various models of clouds. Cloud offerings for various services can be categorized in four different ways. Each one of them can be classified based on their unique features such as: owner of the infrastructure, where it is located, who manages it and who accesses the services of the cloud.

A. Public Clouds

It deals with offering services to the public as an entity. Infrastructure is located at the service provider side who decides all the activities of the cloud along with the owner and managerial rights. As a security paradigm public clouds are considered unsafe as the data is open to the general public and there is no contract agreement with the provider.

B. Private Clouds

It provides services to a particular organization where resource sharing is not done with other organizations**.** Cloud resources are operated purely for a single organization. It is managed by an organization or a third party and may or may not present on provider side. It is considered trustworthy as user has a total control over the service it provides and integrity parameters of his data along with the network route.

C. Community Clouds

It offers services to a group of organizations having the same deployment features as private clouds. It is basically the private cloud for the group of organization with the public cloud features. Users in this cloud are considered trusted by the organizations that are part of the community as in the private cloud also it is the single organization which is allowed to access services.

D. Hybrid Clouds

Hybrid cloud is a combination of above stated clouds. Hybrid clouds contain advantages and features of every deployment model introduced. Hybrid clouds have owner and managerial rights on organization as well as on third party provider side. Also they can be located on either side. Users of this cloud can be both trusted and untrusted. Untrusted users are restricted to access the resources of the private and community parts.

III. CHALLENGES IN ACHIEVING SECURITY

Well proved mechanisms are required to deal with various security issues and to impart safe and efficient service environment in a cloud. Services that are provided to the users must be monitored on usual basis. This monitoring is necessary because of the agreement that is made between the customer and the provider. This agreement is termed as Service Level Agreement (SLA) and it enhances performance of a system. Uniform standardization should be maintained for the agreement. The application interfaces must be easily understood because these are very essential for the providers of service in cloud computing. Cloud data security is more vulnerable to attack due to virtualization because cloud is open and shared in nature[11]. Sharing nature may cause degradation in performance of computing data from the cloud which in turn violates the policy of secrecy.

Therefore, there arises an urgent need to pay attention towards several security issues and introduce some security techniques to handle the problem.

IV. SECURITY ISSES IN VARIOUS SERVICE MODELS

Cloud computing systems actually can be considered as a collection of different services. Framework of cloud computing is divided into three layers: infrastructure layer, platform layer, and application layer[12]. Each one of them provides different services. The various services provided by each layer are:

A. Infrastructure layer

Infrastructure as a service or the hardware related services are provided by the vendors like storage space or the virtual servers. The cloud subscriber is mainly responsible for the data security except the hardware infrastructure. The Example of IaaS is Amazon Elastic Compute Cloud.

B. Platform layer

Platform as a service such that inter-operability is provided among the various platforms provided by the various vendors so that there is a independence regarding the platform like operating system to be used. The security in this model is a shared responsibility of cloud provider and the customer. The Amazon Simple Storage Service is an example of PaaS.

C. Application layer

Application as a service or simply the complete software is provided as a end product to the users of the cloud without using any of the mid services. The service provider is

responsible for the software security in this model. The Google applications and salesforce.com are examples of SaaS.

All the above layers depending on the services it provides to the consumers have various security threats on different parameters which vary according to the layer at which the cloud is working. So according to the services of different layers, security issues caused are addressed in table I.

TABLE I. SECURITY ISSUES IN VARIOUS SERVICE MODELS

Service Models	***Description***	***Examples***	***Security issues***
Software as a Service (SaaS)	It imparts simple software services along with user interface to end user.	Google docs, G mail, Yahoo, Salesforce.com (CRM application) etc.	Privacy of data, Security of network and locality, Integrity and access of data, Authentication, Backup, Availability etc.
Infrastructure as a Service (IaaS)	In this computer framework is treated like a service and the consumer does not purchase the resources instead they buy them.	Amazon web services, Windows Azure etc	1. Taking Virtual machines off creates security challenges. 2. Security issues in operating system are encountered in IaaS.
Platform as a Service (PaaS)	It provides with the deployment of apps without buying and managing the software and hardware for it. To build and deliver web apps Paas provides what all is required.	Google App Engine, SQL Azure etc.	1. Apps are built by users and this control is given to them by the provider. 2. Security of the apps is controlled by the provider only. 3. If hackers can attack the infrastructure of an app they are more likely to attack the visible code of it.

V. EXISTING SECURITY SCHEMES

To overcome the challenges and issues raised various security schemes have been proposed for different issues that are listed below

A. Data Storage Security

Data is stored in data server in cloud computing and data server are remote in nature. Basically companies store data on data server and presume that their data will remain in secure state. However, unauthorized user can gain access to the data residing on remote cloud to alter it, this can cause server to compromise on the matter of correctness of data[13]. To avoid the above problem, a distributed scheme with explicit data storage is provided for modified and lost data recovery.

a) Strengths

Various operations like update, delete, append are carried out easily without the loss of data or without data being corrupted.

b) Limitations

Although the security is well maintained, few issues with data error location still persist.

B. User indentity safety in cloud computing

In this type of technique, user identity is checked over encrypted data that has been sent. Third party is not involved instead active bundle scheme is used.

a) Strengths

The third party here remains free and does not take part in user identity verification.

b) Limitations

All the host might not support the active bundles which has user identity. Therefore, the identity of user is not revealed and user can not have access to data.

C. Trust model for security and interoperability in cross cloud

Here, different domains are used for customer as well as providers and every domain has unique agent called as trust agent. These agents use different trust strategies for each of its user whether it is a customer or a provider. For a good trust various factors like time, accuracy, transactions and integrity are taken into consideration.

a) Strengths

This technique does not allow malicious user to have access to information and hence avoids provider to serve a malicious user.

b) Limitations

Only limited numbers of trust agents are handled because for a provider to avoid sending data to few malicious users is not that easy.

D. Visualized defence and reputation based trust management

It uses DHT hierarchy which is based on networks overlay. Highest layer deals in attacks and lower deals with aggression.

a) Strengths

Virtualization is used extensively for making cloud secure.

b) Limitations

To verify and enhance the performance various simulations are performed because the model is in early development stage.

V. RELATED WORK

In this section, we are going to discuss the literature work done describing the potential threats faced by the clouds.

A survey paper by IDC (International Data Corporation)[14] suggests that cloud services still needs the security parameters to be addressed as an issue and therefore it is not preferable as secure service by the users. There are various security issues that need to be addressed in order to increase its adaptability.

A survey on current services provided by cloud computing [15] is discussed and authors mentioned challenges that must be taken into consideration in order to make cloud computing a success in the field of virtualization.

A research [16] in which various tools for integrity and authentication are discussed. These cryptographic tools ensure solution to some of the security issues but still many of them need further studies. The security solutions mentioned by the Cachin racks various parameters like local copy of the data, Digital Signatures, firewalls etc.

AWS (Amazon Web Services) [17] published a paper which discussed data security, server security, data integrity, authentication certificates. Other providers such as Google, Microsoft etc. have also discussed various security issues that are faced by cloud computing [18].

A paper [19] that identified various indispensable risks that are prominent issues in the security and various parameters that customers must keep in mind in order to utilize cloud computing services.

VI. CONCLUSION

Cloud computing is an extension of existing techniques for computing systems. Various threats from network level to application level are likely to happen in cloud computing and these need to be checked so as to make our cloud more secure. Confidentiality and integrity of data should be maintained so that our data remains secure. This paper tells us about the various security issues and the challenges faced in cloud computing. It also tells us the various objectives that will help to enhance the security of data in cloud. Just like two sides of a coin there are two aspects in cloud computing, on one side high security of data residing in cloud is required and on the other side cloud computing itself give rise to possibility of security attacks. So there is an urgent need to make clouds more secure so as to fulfill the network requirements. Major improvements need to be done in bandwidth that is required to send data over network and increase the capacity of the cloud to hold data.

Security issues and challenges have been briefly described in this paper we should be careful about security of data residing in cloud. Security model should be made with lot secrecy.

References

[1] P. Mell and T. Grance, "The NIST Definition of Cloud Computing", version 15, National Institute of Standards and Technology (NIST), Information Technology Laboratory, www.csrc.nist.gov, (2009) October 7.

[2] Amazon elastic compute cloud (2008), http: aws.amazon.com/ec2/

[3] Twenty Experts Define Cloud Computing (2008) , http://cloudcomputing.syscon.com/read/612375_p.htm

[4] Weiss, A.: Computing in the Clouds. Networker 11, 16–25 (2007)

[5] Barr, J. (2008). The emerging cloud service architecture, from http://aws.typepad.com/aws/2008/06/the-forthcoming.html

[6] Kaleem Ullah,M. N. A. Khan, (2014)On Security and Privacy Issues in Cloud Computing Environment,IJGD,Vol.7, No.2 (2014), pp.89-98 http://dx.doi.org/10.14257/ijgdc.2014.7.2.09

[7] M. Jensen, J. Schwenk, N. Gruschka, and L. Lo Iacono, On Technical Security Issues in Cloud Computing. IEEE, 2009.

[8] Kaufman, L. M. (2009). Data security in the world of cloud computing. Security & Privacy, IEEE, 7(4), 61-64. http://doi.ieeecomputersociety.org/10.1109/MSP.2009.87

[9] Mather, T., Kumaraswamy, S.,&Latif, S. (2009). Cloud security and privacy. Beijing; Cambridge [Mass.]: O'Reilly.

[10] Rittinghouse, J. W., &Ransome, J. F. (2010). Cloud computing: Implementation management, and security. Boca Raton: CRC Press.

[11]] A. Zia, A. Khan and M. Naeem, "Identifying Key Challenges in Performance Issues in Cloud Computing", International Journal of Modern Education & Computer Science, vol. 4, no. 10, (2012).

[12] Subashini, S., &Kavitha, V. (2011). Review: A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications, 34(1), 1-11. 10.1016/j.jnca.2010.07.006

[13] D. H. Patil, R. R. Bhavsar and A. S. Thorve, "Data Security over Cloud", International Journal of Computer Applications® (IJCA), (2012).

[14] Gens, F.: IT Cloud Services User Survey, part 2: Top Benefits and Challenges(2008)

[15] Buyya, R., Yeo, C.S., Venugopal, S., Broberg, J., Brandic, I.: Cloud Computing and Emerging IT Platforms: Vision, Hype, and Reality for delivering Computing as the 5th Utility. Future Generation Computer Systems 25, 599–616 (2009)

[16] Cachin, C., Keider, I., Shraer, and A.: Trusting the Cloud. IBM Research, Zurich Research laboratory (2009)

[17] Microsoft Live Mesh (2008),http://www.mesh.com

[18] Brodkin, J.: Seven Cloud Computing Security Risks (2008),http://www.gartner.com/DisplayDocument?id=685308

[19] Overview of Security Processes (2008).