Data Security on Cloud Computing

Sachin Elaveettil
Department of MCA,VESIT, Mumbai
University Of Mumbai,

Abstract — Cloud computing has come out as a growing trend that has eliminated the difficulties of hardware and software infrastructure by facilitating virtual machines via internet. With 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 are analyzing the various security aspects that are vulnerable to cloud computing and needed to be resolved. It will help to upgrade promising benefits of cloud computing so that consumers cannot have a second thought regarding its adoption.

Keywords — data security; cloud computing;

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 - 2]. 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 distributed on the rent basis as a service, resource or as a platform.

B. Large Scale
To widespread access in terms of storage and range, the computing system includes numerous servers and Computers.

C. Rented service delivery model
Instead of buying hardware and software, users has to pay for the asset on temporary basis.

D. Reliability, usability and extensibility
Cloud storage helps to secure storage of user's data without worrying about the issues like software updation, viruses and data loss.

E. Flexibility
Services can be used anywhere and anytime. And they can be easily scaled up and down.

F. Virtualization
Virtualization helps to virtualize all the infrastructure services. Users can access services with the help of web and can get the data from cloud on rental basis instead of maintaining their own resource pool.

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

The highest layer (public cloud, private cloud, community cloud, hybrid cloud) represents deployment models. The second layer represents service models (SaaS, PaaS, IaaS) [3] that can be utilized as an application service in a particular deployment model. The third and final layer represents important characteristics provided by the cloud.

Cloud computation encounters some security challenges regarding its transmission, storage, authentication, application level security and security related to third party resources [4 - 7]. Challenge changes according to the selected service model.

II. CLOUD DEPLOYMENT MODEL

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

A. Public Clouds
It deals with providing services to the public as an entity. Service provider side who decides all the activities of the cloud along with the owner and managerial rights is where the infrastructure is situated. As a security paradigm public clouds are considered insecure as the data is open to the public and there is no contract agreement with provider.

B. Private Clouds

It offers services to a particular organization where sharing of resources is not done with other organizations. Cloud resources are operated for a single organization. It's handled 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 services it offers and integrity parameters of his data along with the network route.

C. Community Clouds

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

D. Hybrid Clouds

It is a combination of above stated clouds. It contains features of every deployment model introduced. It has managerial and owner rights on organizations as well as on third party provider side. And they can be located on either side. Users of the cloud can be trusted and untrusted. Untrusted users are prevented from accessing the resources of the private and community parts.

III. CHALLENGES IN ACHIEVING SECURITY

Good mechanisms are required for dealing with various security issues and to impart efficient service environment in a cloud. Services offered to the users must be monitored on usual basis. Monitoring is necessary because of agreement that is made between the customer and the provider. Agreement is termed as Service Level Agreement (SLA). It improves performance of a system. Uniform standardization has to be maintained for this agreement. Application interfaces should be easily understood because they are very essential for the providers of service in cloud computing. Data security in cloud is more vulnerable to attack due to virtualization as cloud is open and shared in nature[8]. Sharing may cause the degradation in performance of computing data from the cloud which in turn violates the policy of secrecy. Therefore, there is a rise in urgent need to pay attention towards many security issues and introduce security techniques to handle those problems.

IV. SECURITY ISSES IN VARIOUS SERVICE MODELS

Cloud computing systems can be considered as a collection of various services. Framework of cloud computing is categorized into three layers: infrastructure layer, platform layer, and application layer[9]. Each one provides different services. The services provided by each layer are:

A. Infrastructure layer

Infrastructure as a service is provided by the vendors like the virtual or servers storage space. The cloud subscriber is responsible for data security except the hardware infrastructure. Amazon Elastic Compute Cloud is an example.

B. Platform layer

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

C. Application layer

Application as a service is provided as an end product for the users of cloud without using any of the mid services. Service provider is responsible for software security in this model. Examples of SaaS are Google applications and salesforce.com.

Above layers depending on the services provided to the consumers have various security threats on different parameters which vary according to the layer at which cloud is working.

V. EXISTING SECURITY SCHEMES

For overcoming the issues and challenges various security schemes are proposed for different issues that are listed below:

A. Data Storage Security

Data are stored in data server in cloud computing. And data servers are remote in nature. Companies store data on data server and assume that the data will remain in secure state. Unauthorized user can gain access to the data residing in remote cloud to alter it. This can cause server to compromise on the matter of correctness of data[10]. To avoid this problem, a distributed scheme with explicit data storage is offered for modified and lost data recovery.

a) Strengths

Different operations like append, update and delete can be carried out easily without data being corrupted or without any loss of data.

b) Limitations

Even if the security is well maintained, some issues with data error location still persist.

B. User identity safety in the cloud computing

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

a) Strengths
Third party here remains free and do not take part in the verification of user identity.

b) Limitations
Every host may not support the active bundles which has user identity. Therefore, user identity is not revealed and therefore, user can not have access to the data.

C. Trust model for security and interoperability in cross cloud
Different domains are used for customer as well as providers and each domain has unique agent called trust agent. Agents use various trust strategies for each of its users whether it is a customer or a provider. For trust various factors like time, accuracy, integrity and transactions are taken into consideration.

a) Strengths
This technique don't allow malicious user to have access to data and information and hence avoids provider in serving a malicious user.

b) Limitations
Limited numbers of trust agents are handled because for a provider to avoid sending data to very few malicious users isn't easy.

D. Visualized defence and reputation based trust management
This technique uses DHT hierarchy which is based on networks overlay. Highest layer deals with attacks and lower layer deals in aggression.

a) Strengths
Virtualization is used for making cloud secure.

b) Limitations
To enhance and verify the performance various simulations are performed as the model is in its early development stage.

VI. RELATED WORK

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

A survey paper by IDC[11] suggests that the cloud services needs the security parameters to be addressed as an issue and therefore it's not preferable as a secure service by the users. There are many security issues that must be addressed in order to increase its adaptability.

A survey on the current services offered by the cloud computing [12] is discussed and authors mentions the challenges that must be taken into consideration to make cloud computing a success in field of virtualization.

A paper published by AWS (Amazon Web Services) [13] in which it discussed data security, server security, data integrity, and authentication certificates. Other providers such as Google, Microsoft etc. have discussed different security issues that are faced by cloud computing [14].

A research [15] in which different tools for authentication and integrity are discussed. Those cryptographic tools make sure solution to some security issues but still many of them need further studies. Security solutions mentioned by Cachin racks various parameters like local copy of data, Digital Signatures, and firewalls etc.

A paper [16] which identifies various indispensable risks that are prominent issues in the security and parameters that customers must keep in mind for utilizing cloud computing services.

VII. CONCLUSION

Cloud computing is an extension for existing techniques of computing systems. Different threats from network level to application level can happen in cloud computing and it needs to be checked so as to make cloud secure. Integrity and confidentiality of data is maintained so that our data remains secure. This paper tells us about the different data security issues and the challenges faced in cloud computing. It tells us the various objectives which will help in enhancing the security of data in the cloud. Just like two sides of a coin there are two aspects of cloud computing, on one side data security in cloud is required and on the other side cloud computing give rise to possibility of security attacks. So there's an urgent need for making clouds more secure so as to fulfil the network requirements. Major improvements needs to be done in bandwidth that is required to send data over network and increase capacity of cloud to hold the data.

Data Security issues have been briefly described in this paper and we should be careful about security of data residing in cloud storage.

REFERENCES

[1] Weiss, A.: Computing in the Clouds. Networker 11 (2007)

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

[3] On Security and Privacy Issues in Cloud Computing Environment, Kaleem Ullah,M. N. A. Khan, (2014) , IJGD,Vol.7, http://dx.doi.org/10.14257/ijgdc.2014.7.2.09

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

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

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

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

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

[9] Review: A survey on security issues in service delivery models of cloud computing, Subashini, S., &Kavitha, V. (2011). [10] Data Security over Cloud, D. H. Patil, R. R. Bhavsar and A. S. Thorve, International Journal of Computer Applications® (IJCA), (2012).

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

[12] 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) ,Buyya, R., Yeo, C.S., Venugopal, S., Broberg, J., Brandic, I.:

[13] Microsoft Live Mesh (2008)

[14] Seven Cloud Computing Security Risks by Brodkin

[15] Trusting the Cloud. IBM Research, Zurich Research laboratory (2009) Cachin, C., Keider, I., Shraer, and A.(2008),http://www.gartner.com/DisplayDocument?id=685308

[16]Overview of Security Processes (2008)