International Journal of Engineering Applied Sciences and Technology, 2016
Vol. 1, Issue 6, ISSN No. 2455-2143, Pages 67-69
Published Online April - May 2016 in IJEAST (http://www.ijeast.com)

SECURITY IN CLOUD COMPUTING

Shweta Kaushik
Department of Computer Science & Information Technology
Jaypee Institute of Information Technology,
Noida, U.P, India

***Abstract*— Today many individual and organizations are moving toward cloud computing for storing their large amount of data over distributed system with the ease of accessing data at anytime and anywhere. Cloud computing relax the user from data accessing, processing and its storage and maintenance as all these task are related to service provider who is completely responsible for this. But, security of confidential data is a prime concern of data owner .To makes it free from any unauthorized user access, alteration etc. owner can encrypt the data before transmit it over cloud system as service provider is also an un-trusted party who can also utilize the owner data for its own benefit. This paper provide basic introduction of cloud system and present the various work done by researchers to secure the data from any malicious activity in cloud system.**

Keywords—**Cloud computing, Public cloud, Private Cloud, Security**

I. INTRODUCTION

A. Cloud Computing

Cloud computing is a rapidly growing technology which allows the user to easily access and use the required services and information stored at remote location which can be accessed via internet. It is a pool of shared resources such as storage, network infrastructure, application and services on a distributed network. It is useful for organization or individual to access the data, resources and services on the pay-per-use basis, that is user has to pay only for the amount of data, resources and services which are used by an organization or individual and not for entire data, resources and services. One of the prominent features of cloud computing is that the user's data is stored at some remote location, i.e. cloud. The cloud service provider is responsible for the data maintenance and security. The cloud is owned by the cloud service provider whereas the data operations are controlled by the data owner. Today many organizations based on education, healthcare and banking domain are moving towards cloud to provide various services to their clients on the pay-per -use basis. Some of the major cloud service providers are Google, Amazon, Salesforce, etc.

B. Cloud User

There are generally three entities involved in the concept of cloud computing.

Owner- Owner is the one who has the data, resources or services which is needed by the user. Owner stores all the data, resources and services on the cloud from where user can access them. Owner decides the type and level of the access to the user on data, resources or services.

Cloud service Provider (CSP)- CSP act as an interface between the owner and the user. CSP is the one who maintains the data, resources and services and setup the security protocols. CSP allows the authorized user to access this data, resources and services on the basis of some criteria decided by the owner which is based on the role, capability, access control, authorization, etc.

User- User is the one who required the data, resources and services and gets it from the cloud service provider according to his requirement and pay only for the amount of data or resource used by him.

C. Cloud Deployment models

According to the development of cloud in various organizations and for social usage, it can be classified as-

Public Cloud- It is an infrastructure provided to the user or many organizations in order to utilize the various available resources without any firewall implementation to deliver the cloud data. This type of model is managed and provided by the third party who is responsible for handling all the request and issues. There is no access restriction, authorization and authentication mechanism.

Private cloud- It is an infrastructure which is provided within an organization to utilize its resources under the firewall implementation. This type of model is either owned or leased from a third party and managed by the organization to deliver the resources to the user according to the security criteria such as access control, authentication etc.

Hybrid cloud- This type of infrastructure is a combination of two or more deployment models, in such a manner that the data transfer between them does not affect each other i.e. formed with the both private and public.

D. Cloud Delivery models

On the basis of which type of services provided by cloud, it can be classified as-

Software as a service (SaaS)- It can be defined as delivery of various software and application to the user on the internet according to the requirement and allow to use, maintain and operating them at the server virtually without installing any software on the user's machine. Example- salesforce.com, Google Apps

Platform as a service (PaaS)- It can be defined as delivery of the computing services such as operating system, database program execution environment to the user which allows them to implement and execute their program or application over the internet without any need to install anything on the user's machine and also maintained on the cloud. Example- Force.com, Microsoft Azure.

Infrastructure as a service (IaaS)- It can be defined as delivery of hardware resources to the user according to the requirement of the user using virtualization to execute their application. Example- Amazon EC2, GoGrid

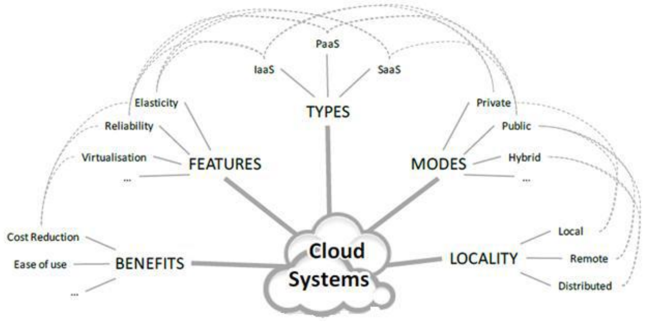

Fig. 1 Cloud computing

E. Cloud Security

In cloud computing, data is stored at some remote location and it is the cloud service provider's responsibility to organize and maintain this data, without any data leakage. Owner of the data does not have any copy of this data and is also not responsible for securing this data from leakage, hack, etc. Since the cloud service provider is an external entity, the owner cannot completely trust service provider to secure its sensitive data which is allowed to be accessed by only authorized party. There is a need of security steps, algorithms and protocols, so that data can be in encrypted format at the cloud service provider's end and without any access to the key to decrypt the data. Only authorized user has the key to decrypt the data received from the cloud service provider to convert the data into meaningful information.

II. SECURITY REQUIREMENTS

Table 1
Cloud computing Security Requirements

S.NO	Security Requirement	Description
1	Confidentiality	Security requirement in which the message must be correctly interpreted by the intended user. To do this, unauthorized access and usage must be prevented.
2	Authenticity	Security requirement in which the nodes in the network should dispatch its intended services without fail.
3	Integrity	Security requirement in which messages should not get modified while transferring between sender and receiver.
4	Authenticity	Security requirement ensures the identity of node with which communication takes place is genuine.
5	Authorization	Security requirement to ensure that information dissemination should only from authorized sensors.
6	Non repudiation	Security requirement deals with retransmitting of message by a node. A node should not deny retransmitting of already sent message.
7	Freshness	Security requirement deals with maintaining and disseminating up to date information by sensor nodes.

III. RELATED WORK

Table 2
Literature integration

Functionality	Description
Secure cloud data storage with access control and assured deletion[1]	All the process related to the access, key management and deletion of a particular file are managed by a quorum of key management. Policy based access control, deletion. Use of threshold secret sharing.
Manage data retention policies outside cloud system[2]	Permanent deletion of data from storage by just only removes their encryption key. Deletion of an encryption key ensures that replicated data will be of no use. A key management store, for distributing the fragment or a portion of the key store to the various parties.
Enabling dynamic data and indirect mutual trust for cloud computing storage systems[3]	An indirect trust is maintained between the data owner and cloud service provider. If any dispute arises then it will be handled by trusted third party. Provides safeguards to the service provider from the owner, as the owner does not claim false regarding the data corruption.
Key management scheme for cloud data protection[4]	All the data during its transmission is encrypted using the session key, which ensures high security. If there is any modification done in the cloud hierarchy it will not affect the data security. User private key used for encrypting the data is not stored on the cloud system.
Mutual Trust Based Access Control Model in Cloud Computing[5]	User can select the most convincing cloud service node to acquire the required resources or process. The trust is calculated in two modes- (i) user behavior (ii) trust calculation of the cloud service node. User behavior trust is calculated using the

	analytic hierarchy process. The cloud service node trust model is based on ant colony optimization algorithm.
Role-Based Access Control on Encrypted Data in Cloud Storage[6]	A secure cloud data storage architecture using a hybrid cloud infrastructure, where the private cloud is used to store only the organization's sensitive structure information and the public cloud is used to store the actual data that is in the encrypted form. A user is able to join a role after the owner has encrypted the data for that role. The interaction of the user to get the required encrypted data and of the owner who want to encrypt the data is done through only public cloud to secure the sensitive data which is stored in private cloud.
Attribute-based trust model for service level agreement guarantee in cloud computing[7]	Provides a way to select any service provider objectively rather than subjectively rating on the basis of predefined attribute. Adaptive model to measure trust according to multi-dimensional attribute. SLA is a contract signed between parties to maintain and evaluate the service according to this and provide a guarantee.
Information Flow Control (IFC) for secure cloud computing[8]	Security policies are defined in agreement of both, tenants and providers which reduce the need of outsider cloud stack for enforcement. System does not pose any overhead as cloud developer/ provider is aware of trust inherent in IFC system. The IFC system provides security by introducing the label at data and principal and shows their relationship.
Secure Logging as a Service[9]	Use the anonymous network which does not require knowing whose log records are shared in the logging cloud. Use of proactive secret sharing scheme neglects the chance of any outsider to interlink the log record to the logging client. If any attacker tries to breach the security policies, logging cloud can easily catch it because every uploaded tag has a unique timestamp associated with it.
Public audit ability and data dynamics for storage security[10]	Third Party Auditor (TPA) allows verifying the integrity of the remote data without acquiring any knowledge of exactly what data is. Support of dynamic operation makes it useful for the user to easily modify its data according to change requirement. Use of homomorphism authentication generates metadata which is useful for the verification of the data.

IV.CONCLUSION

In recent year, cloud computing is an auspicious solution to provide the resources to the user in an effective and efficient manner, within budget limitations and anywhere via Internet. But one of the obstacles for cloud computing use is its security concern. User stores their data at remote location, without any physical access to the data. It raises a question whether the data is safe from malicious activities or not, what security policies are defined for that? To resolve these problems, there is a need to provide proper security model, which consider all these issues and secure the data on cloud from malicious activities.

V. REFERENCE

[1] Tang, Yang, et al. "Secure overlay cloud storage with access control and assured deletion." Dependable and Secure Computing, IEEE Transactions on9.6 (2012): 903-916.

[2] Li, Jun, et al. "Managing data retention policies at scale." Network and Service Management, IEEE Transactions on 9.4 (2012): 393-406.

[3] Barsoum, Ayad, and Anwar Hasan. "Enabling dynamic data and indirect mutual trust for cloud computing storage systems." Parallel and Distributed Systems, IEEE Transactions on 24.12 (2013): 2375-2385.

[4] Kao, Y-W., et al. "uCloud: a user-centric key management scheme for cloud data protection." Information Security, IET 7.2 (2013).

[5] LIN Guoyuan, WANG Danru, BIE Yuyu, LEI Min. "MTBC: A Mutual Trust Based Access Control Model in Cloud Computing" China Communication in April (2014): 154-162.

[6] Zhou, Lan, Vijay Varadharajan, and Michael Hitchens. "Achieving Secure Role-Based Access Control on Encrypted Data in Cloud Storage." (2013): 1947-1960.

[7] Xiaoyong Li, Junping Du. "Adaptive and attribute-based trust model for service level agreement guarantee in cloud computing." IET Inf. Secur., 2013, Vol. 7, Iss. 1, pp. 39–50 (2013): 1947-1960.

[8] Bacon, Jean, et al. "Information Flow Control for secure cloud computing." IEEE transaction on network and service management, vol. 11,issue 1, march 2014,pp. No 76-89.

[9] Ray, Indrajit, et al. "Secure Logging as a Service---Delegating Log Management to the Cloud." IEEE systems journal 7 (2013): 323-334.

[10] Wang, Qian, et al. "Enabling public auditability and data dynamics for storage security in cloud computing." Parallel and Distributed Systems, IEEE Transactions on 22.5 (2011): 847-859.