IJCSE International Journal of Computer Sciences and Engineering Open Access
Survey Paper Volume-2 Issue-8 E-ISSN: 2347-2693

Secure Cloud Storage with Access Control: A Survey

Ms. P.Ranjima[1*], Ms. Sumathi. D[2] , Ms.Minimol Mathew[3] and Mr.P.Sivaprakash[4]

[1*,2,3,4]*Dept of CSE, PPG Institute of Technology*
www.ijcseonline.org

Received: 23 Aug 2014 Revised: 04 Sep 14 Accepted: 29 Aug 2014 Published: 05 Sep 2014

Abstract- Cloud computing is a technique used to refer web based services and development. It is a ubiquitous services, means anyone can access from anywhere in the world at anytime. It provides application, platform and resources to the user. It is a virtualized pool of resources. These services are provided by CSP. The main features of cloud are flexibility, elasticity, on-demand services, metered services, etc. Some large companies offer data storage spaces which are leased to others. So the devices connected to internet can achieve these services. Cloud stores data in database and replicated in different virtual machines, that can be placed anywhere in world. This may leads to some major security issues in cloud storage and retrieval. In order to prevent unauthorized access, access control techniques can be used. A user authentication verifies identity of user. While providing services; we are concern about security and privacy of the information. This survey paper introduces a detailed analysis of security and privacy preserving techniques, and a comparison among various access control mechanism.

Keywords- Cloud computing; Security; Attribute Based Encryption; Authentication; Access control

I. INTRODUCTION

Cloud computing is an internet-based service, where hardware resources, software, application and information are shared and provided to users. It is an environment created in user machines from an online application, stored on cloud and run through a web server. Cloud is used to access someone else's software on someone else's hardware in someone else's data centre. The important advantages of this model are ease-of-use and cost- effectiveness. Hence industrial experts prefer cloud for their storage and research[16].

Cloud varies based on services offered. According to different services offered to cloud computing, it has three layers: such as Infrastructure as a Service(IaaS), Platform as a Service(PaaS) and Software as a Service(SaaS)[4].

IaaS is the lowest layer that provides basic infrastructure for services. Examples are Amazon's EC2, Eucalyptus, Nimbus,etc. PaaS is the middle layer offers platform and hosting environment for services. Well known examples are Amazon's S3, Windows Azure,etc. SaaS is the top most layers that provide entire service or application. Some application services are Google Apps, Microsoft online,etc.

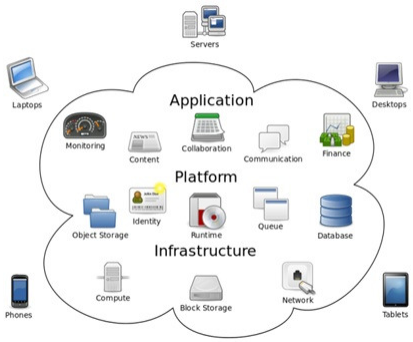

Fig: Cloud Computing

Based on deploy application used in cloud computing it can be divided into three types: public cloud, private cloud and hybrid cloud.

- **Public cloud:** In pubic cloud, cloud venders provide infrastructure and can share in various organizations. Examples are Google, Amazon, Microsoft, etc.
- **Private cloud:** Here infrastructure is provided to trusted users and organizations and does not share by other users and organization. It is more expensive and secure. Examples are IBM, Oracle, HP data centre, etc.
- **Hybrid cloud:** Usage of both public and private cloud together is called hybrid cloud. Here service providers can utilize third party providers in a full or partial manner, hence increases the flexibility of computing.

II. SECURE DATA STORAGE IN CLOUD

Many clouds offer storage as a service, i.e. they retrieve data from users and stores in them large data. While storing data in cloud, we should concern about security of data stored. For secure storage of data in cloud we are considering identity management, physical security, personnel security, application security, and privacy.

Data can be stored either in a centralized or decentralized manner. In a centralized structure, data kept in a centralized storage. But there is a chance of single storage failure. While a decentralized structure data can be stored in distributed storage spaces. So chance of failure is comparatively less. So a decentralized structure provides security compare to centralized structure.

Cloud has an important behaviour called virtualization. It provides an environment for all services and provides hardware, ie personal computers to the end users. Some categories of existing systems are Storage virtualization, CPU virtualization, I/O virtualization and

Memory virtualization. Hence for virtualized storage traditional security issues handling mechanisms are inefficient.

Normally data which is preserved safely by various encryption techniques, such as: public key encryption and private key encryption. A homomorphic encryption method is widely used for encryption and decryption. Similarly a newly developed attribute based encryption method is also used instead of these techniques.

According to W.Wang,Z.Li, R.Owens and B.Bhargava, they provide a centralized structure for data storage. Their paper[7] Provides a secure and efficient access to outsourced data. Also they solve the problem of owner-write-users-read applications. In order to provide access control on basis of cryptography, use different keys for encrypting every data block. But it takes a lot of time for key generation. But hash function needs a limited computation for key generation.

Hence using hash function encryption is performed. It provides an access control mechanism. To prevent invalid user from accessing data an over encryption schemes is performed. Using a pseudorandom bit sequence generator these operations held. But it does not preserve identity of users. Here it handles both updates to outsourced data and changes in user access rights.

According to S.Ruj, A.Nayak and I.Stojmenovic in their paper [2], they propose for decentralized storage and access control mechanism. The process of granting access rights to certain users and avoiding access of unauthorized users is known as access control mechanism [5]. In order to grant access to users, there are three methods available. First method is attaching list of all valid user with data. Here in each time the list has to be checked to see if the user is valid. Hence it needs huge computation and storage cost. Second is encrypting data using public key of valid users. There is a problem to faced, each time the list has to be checked to see if user is valid. It may result in huge storage cost. Last method is Attribute Based Encryption (ABE), here owners encrypted data with attributes that they possess and store the information in the clouds.

Here data encrypted using ABE by owner and user receives decryption keys. KDC used for secret key distribution. KDCs which may be even servers scattered in different countries. And [2] provides two format of access policies like Boolean function of attribute and Linear Secret Sharing Scheme (LSSS). Their access control mechanism is safe and allows access only to authorized users. Here user verifies data authentication and preserve their identity and simultaneously provides user authentication [8].

According to Kan Yang, Xiaohua Jia and Kui Ren , because of data outsourcing and suspicious cloud servers, data access control becomes worst. And existing techniques produce a multiple number of encrypted copies. Hence [3] provides a decentralized and an attribute based encryption technique for access control. A Ciphertext-Policy Attribute-based Encryption (CP-ABE) is used. A CP-ABE method provides an efficient decryption technique. It is the type of identity-based encryption. It uses one public key and a master key that is used to generate several restricted private keys. The main computation of the decryption is the usage of a token based decryption method. Moreover, CP-ABE is more flexible than identity-based encryption, in that it allows complex rules specifying which private keys can decrypt which cipher texts [9]. Specifically, the private keys are associated with sets of attributes or labels, and when we encrypt, we encrypt to an access policy which specifies which keys will be able to decrypt [10].

Also it provides an efficient user and attribute revocation method that achieves both forward security and backward security. Whenever a user is revoked then he can't access associated file anymore. But it does not preserve the identity of users. This is the main problem occurred in this paper.

According to S.Yu, C.Wang, K.Ren, and W.Lou, they focus on important issues of user revocation which is the difficulties for CP-ABE. In [6] it provides a centralized structure for cloud storage. Here they resolved these challenging issues by considering practical scenarios. We know that CP-ABE uses a public key and a master key that is used to generate restricted private keys. It defines a master key for each attribute of a system. While using master key, the system defines public key and secret key of user's attributes.

When an attribute revoked, authority redefines master key related to that attributes. A public key is generated simultaneously for that master key. Using that public key, data can be decrypted efficiently. Similarly secret key is generated simultaneously for data access and decryption. Similarly [6] it is based on user revocation and it places minimum load. This is achieved using CP-ABE with proxy re-encryption techniques. Similarly there is no authentication mechanism available for preserving privacy of user and identity is not preserved.

According to Sushmita Ruj, Milos Stojmenovic et al., they provide a decentralized access control for secure data storage and it verifies authentication of user. In this paper [1], authorized users only can store, access and modify data stored in cloud. And privacy of user is preserved. Actually cloud does not know the identity of user before storing. It protects the identity of the user.

The decentralized architecture provides several KDC for key management. So it avoids single-point-failure. Similarly it addresses user revocation. Also it prevents access of data by revoked user. A valid data transmission is maliciously or fraudulently repeated or delayed in a network is called replay attack. It prevents these replay attacks.

Table: Comparison among various access control schemes and authentication

Ref No	Centralized/ Decentralized	Type access control	Privacy preserving authentication	User Revocation
[1]	Decentralized	ABE	Identity is preserved	Yes
[2]	Decentralized	ABE	No Authentication	Yes
[3]	Decentralized	ABE	Not Privacy Preserving	Yes
[6]	Centralized	ABE	No Authentication	No
[7]	Centralized	Symmetric key cryptography	No Authentication	No

III. CONCLUSION

A cloud is the practice of using a network of remote servers hosted on the Internet to store, manage, and process data, rather than a local server or a personal computer [15]. A cloud provides infrastructure, platform, application or storage as a service [17]. While storing a data on cloud a decentralized structure is more efficient. In order to provide an access control, an attribute based encryption can be used. Also, while storing the data, identity of the user should be preserved. Similarly it addresses user revocation.

IV. REFERENCE

[1].Sushmita Ruj, Milos Stojmenovic et al.,"Decentralized Access Control with Anonymous Authentication of Data Stored in Clouds", in IEEE transactions VOL:25 NO:2 2014.

[2].S. Ruj, A. Nayak, and I. Stojmenovic,"DACC: Distributed access control in clouds," in IEEE TrustCom, 201 1.

[3].Kan Yang, Xiaohua Jia and Kui Ren,"DAC-MACS: Effective Data Access Control for Multi-Authority Cloud Storage Systems",IACR Cryptology ePrint Archive,419,2012.

[4]www.tcs.com/SiteCollectionDocuments/White%20Papers/HighTech_Whitepaper_Windows_Azure_09_2011.pdf

[5] http://www.w3.org/TR/2007/WD-access-control-20071001/

[6] S.Yu,C.Wang,K.Ren, and W.Lou,"Attribute based data sharing with attribute revocation," in ACM ASIACCS, pp. 261–270, 2010.

[7] W.Wang,Z.Li,R.Owens,and B.Bhargava, "Secure and efficient access to outsourced data," in ACM Cloud Computing Security Workshop ,2009.

[8] www.iosrjournals.org/iosr-jce/papers/Vol9-Issue2/E0922831.pdf

[9] mslab.kaist.ac.kr/twiki/pub/ContentNetworking/WebHome/L26_AC_DRM.pptx

[10] http://psrcentre.org/images/extraimages/1112106.pdf

[11] Seny Kamara, Kristin Lauter, "Cryptographic cloud storage", Lecture Notes in Computer Science, Financial Cryptography and Data Security, pp. 136-149, vol. 6054, 2010.

[12] Kuyoro S. O., Ibikunle F. & Awodele O, "Cloud Computing Security Issues and Challenges," in IJCN, Vol 3 :Issue (5) : 2011

[13] Abhinay B.Angadi, Akshata B.Angadi, et al., "Security Issues with Possible Solutions in Cloud Computing-A Survey," in IJARCET, Vol 2, Issue 2, Feb 2013.

[14] Ritesh G. Anantwar, Dr. P.N. Chatur, et al., "Cloud Computing and Security Models: A Survey," in IJESIT,Vol 1, Issue 2, Nov 2012

[15] Torry Harris, "CLOUD COMPUTING – An Overview,"

[16] http://www.slideshare.net/dattudharanikota/cloud-computing-ppt-14857120

[17] http://en.wikipedia.org/wiki/Cloud_computing

