ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 1, January 2017

Review on Access Control Issues in Cloud Computing

Mallika Roy, Prof. Ashok Verma

Research Scholar, Gyan Ganga Institute of Technology and Science, Jabalpur [M.P] India

Associate Professor & HOD, Dept. of Computer Science Gyan Ganga Institute of Technology and Science Jabalpur [M.P] India

ABSTRACT: Data security issue is a key bottleneck restricting the application of cloud computing promoting and applications. In this paper, states of the art of the techniques on cloud computing data security issues, such as data encryption, access control, integrity, authentication and other issues is surveyed, on this basis, some important technical issues of the cloud computing data security should concern about and focus on are indicated. Cloud computing is the use of computing resources like hardware and software that are delivered as a service over a network. It confides remote services with a user's data and software, it enables a user to do large amount of storage, large amount of computations. Due to which data security in cloud becomes a big issues. Data access control provides the security of data in the cloud. The large amount of data outsourced in cloud servers, the data access control becomes a challenging issue in cloud storage systems. We have many access control security solution like Attribute based, Role based, Hierarchical identity management, Identity based authentication, Trust based model etc. Cloud computing is one recent technologies. So it becomes very necessary to secure the data as well as privacy of users. Access Control methods provide an effective way to ensure that authorized user's access the data and the system. In this paper we discussed various features of attribute based Encryption, Role based, Hierarchical identity management, Identity based authentication, Trust based model suitable for cloud computing environment.

KEYWORDS: Cloud issues, Hierarchical identity management, Encryption, Data access control, Attribute based Encryption, Role based Encryption, Fine-grained Access Control, and Scalability.

I. INTRODUCTION

The great innovation in the field of computing is storage and access of data in the cloud, however, there are many things that need to take care about too. Many authors told that cloud computing has several benefits as compared to their down sides. But we found that as involvement of data increases security of data becomes a huge issues although we need to find a way all you need with a particular service.

Cloud Computing Associated Problems:

A. LOSS OF TRANSPARENCY AND CONTROL OVER THE DATA.

Consumers are unaware of the data loss which is out of their hands and storing data in the Cloud service provider [1]. Confidential data are stored in cloud could be compromised by the user. Due to lack of transparency, the user don't know where, how, when the data is processed. To resolve this problem the user should know what happens with the data. Cloud service providers are technically able to do data mining as well as data abstraction need techniques to analyze user data. So the users can store and process the data in cloud using Cloud service provider. Loss of transparency can also leads to loss of huge amount of data. So unable to trust the cloud service provider.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 1, January 2017

B. LACK OF TRUST AND DEPENDENCE ON CLOUD PROVIDER

A major problem in cloud service provider is availability. Due to lack of fund, the Cloud service provider were stopped providing services, the user could suffer problems in accessing the data. Some widely used Cloud service provider (e.g. Google Drive) does not provide any contract between the user and Cloud service provider.

If any problem or incident arises, users have no proof to ask. Cloud service provider provides services similar to other traditional services and utilities. The customers usually depend on the providers because it is difficult to change providers if it is possible at all.

II. EXISTING SECURITY SOLUTIONS

Now we going to discuss about existing security solutions available for access control mechanism.

A. IDENTITY BASED AUTHENTICATION

Identity based encryption is a public key techniques, where Private Key generator generates master public key and master private key, where master public key is created by user unique information. The user can decrypt the file by getting the private key with his identity from private key generator, by using that he can decrypt the file[1]. Private Key generator not only generates the private keys but also verify the user identities. The main drawback in Identity based encryption is need to trust the private key generator since it holds all private key and must remain online.

B. ROLE BASED MODEL

Data owner before storing the data in cloud, first they encrypt the data in local system and then store the encrypted data in the cloud. Data users can't directly access the data from cloud. Each users are assigned with roles and responsibility. The roles are assigned based on the responsibilities and qualification. The authenticate users have privileges to access the data with specific roles. The users are assigned with different roles and each of them are having a set of permissions. A role manager responsibility is to assign a role to the user, and if the user is going out, then revoke a role from the user. Cloud Provider, users and others are not able to see the data if they are not assigned with proper roles. Data owner can revoke the role if they found as unauthorized user.

C. ATTRIBUTE BASED ENCRYPTION

Before storing the data in the cloud, the data owner encrypted the data in his local system and its decrypted by the data user [2]. In attribute based encryption scheme, set of attributes are treated as user identity and its used for encryption and decryption techniques. Trusted agent generates keys for data owner and user. It generates key according to the attributes of the user [4]. The trusted agent will generate public key and master keys for the user. Data owner role is to encrypt the data with user public key and user will decrypt the data with own private key. We have two advantages in this scheme 1) it reduce communication overhead in the internet 2) Provide fine grained access control. Problem behind in this technique, the data owner need to use the authorized user public key for encryption [3].According to attribute based encryption the access policy is classified into two types key- policy attributes based encryption and ciphertext-policy attributes based encryption.

D. KEY-POLICY BASED ENCRYPTION

In key-policy attribute-based encryption, Ciphertext is associated with set of attributes, Private Key which is issued by trusted authority is associated with access structure like a tree, which describes this user's identity. The user can recover the file if and only if access policy in the private key is satisfied with the attributes in the ciphertext.

The Trusted authority issues the user key, by using access policy we can identify which types of encrypted data can decrypt, while encrypted data are labeled with set of attributes [6]. The drawback in KP-ABE scheme is that data owner dont know who can decrypt the data. The data owner want to trust the key issuer, so its not suitable for some application. Another disadvantage is lack of scalability dealing with levels of attribute authority. To overcome this issue we are moving to ciphertext policy –attribute based encryption.

A set of attributes in the encrypted data {Hospital, Doctor, Patient}, Private key with attribute {Hospital, Doctor} to decrypt and obtain the data.. Eg: Encrypted data with attribute are {Hospital^Patient},and user private key with access structure is {Hospital^(Doctor OR Patient)}

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 1, January 2017

E. CIPHERTEXT POLICY BASED ATTRIBUTES BASED ENCRYPTION

In CP-ABE, the private key is associated with a set of attributes, and a ciphertext are created with access structure, which is used to specify the encryption policy. A user can decrypt the ciphertext if and only if the attributes in the private key is satisfied the access tree specified in the cipher text[7].In CP-ABE scheme, attribute management and key distribution are managed by the authority (eg authority may be registration office in university , Human Resources in company, etc). The data owner defines the access policy and encrypts the data with access policies. Each user is issued with secret key according to its attributes [8].Here data owner holds the ultimate authority about the encryption policy.

Access structure in Encrypted data is {Hospital AND (Doctor OR Patient)}and set of attribute in user's private key is{Hospital AND Doctor} the user can recover the data.

F. HIERARCHICAL ATTRIBUTE BASED ENCRYPTION

Hierarchical attribute based encryption is combination of hierarchical identity based encryption(HIBE) and ciphertext-policy attribute based encryption(CP-ABE). It support full delegation and fine grained access control over attributes.it support one-to-many encryption. Encrypted file can be decrypted by a user and all his family members, using their own secret keys. HABE hold the property of hierarchical generation of keys in the HIBE system, and the property of flexible access control in the CP-ABE system.

G. HIERARCHICAL ATTRIBUTE SET BASED ENCRYPTION

Hierarchical attribute-set-based encryption (HASBE) scheme for access control in cloud computing. HASBE extension of the CP-ASBE, or ASBE scheme with a hierarchical structure of system users, so as to achieve scalable[10], flexible and fine-grained access control. Each data file is associated with a set of attributes, and each user assign with expressive access structure. HASBE employs multiple value assignments for access expiration time to deal with user revocation more efficiently than existing schemes. User can retrieve the encrypted data by using their own private key. These domain authorities monitor the users for their respective acceptance of correct key [11]. A Master-key provided by higher level authorities to manage lower level authority's data. Enforcing access policies based on data attributes and on the other, the data owner to delegate most of the computation tasks involved in fine-grained data access control [12] to un-trusted cloud servers without disclosing the underlying data contents. We achieve this goal by combining techniques of attribute-based encryption (ABE), proxy re- encryption, and lazy re-encryption. The HASBE method flawlessly integrates a hierarchical structure of scheme customers by concerning an allocation algorithm to ASBE. HASBE maintains compound attributes which attains efficient user revocation because of multiple value assignments of attributes. Several methods utilizing attribute-based encryption (ABE) suffer from hardness in implementing complex access control policies [9]. The trusted authority is accountable for generating and distributing system parameters and root master keys as well as authorizing the top-level domain authorities. A domain authority distributes the key to sub domain authority or user. Each user is assigned with key structure which specifies the attribute associated with the user decryption key. Main drawback in this system is deriving unique access structure for each user introduces heavy computation overhead.

I. MULTI AUTHORITY

Multi-authority CP-ABE is more suitable for data access control, multiple authorities issued the attributes to users and using access policy the data owner share the data defined over attributes from different authorities. In this technique, users' attributes can be changed dynamically. A user may be designate with new attributes or revoked some current attributes, then data access should be changed accordingly. Each data owner before encrypting the data, they divide the data into different parts and each parts is encrypt with contents keys by using symmetric encryption techniques. Then, the owner defines the access policies over attributes from multiple attribute authorities and encrypts the content keys under the policies. Once data are encrypted and its send to cloud server with the ciphertext [13]. The server does have option to access the data, and the User can decrypt the data if and only if user attributes satisfy the access policy defined in the ciphertext.

Table shows the limitations of the different authentication techniques using the above discussed security parameters.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 1, January 2017

Comparison of various authentication techniques [5]

Authentication Technique	Security from insider attack	Presence of authentication towards	Extra hardware software needed	No. of security tiers
Authentication using Single –Sign On (SSO) [14]	**No**	**Server**	**No**	**1**
Multi-level authentication [2]	**Yes**	**Server**	**No**	**More than 1**
Architecture based on proactive model[15]	**No**	**Server and Client**	**Yes**	**1**
2-tier architecture with maximized RIA[16]	**No**	**Server and Client**	**No**	**2**
Strong user authentication framework[3]	**Yes**	**Server**	**No**	**2**
Multi-tier security feature model[17]	**No**	**Server**	**No**	**2**
SSO authentication model using Kerberos	**Yes**	**Server and Client**	**No**	**2**
Anonymous Password Authentication Scheme[19]	No	Server	Yes	2
Mutual Authentication Framework[20]	No	Server and Client	Yes	2
Multi-tier Authentication Scheme[5]	Yes	Server and Client	No	2

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 1, January 2017

III. CONCLUSION

Access control security is one of the important issues in cloud. Better access control protects cloud system from security problem. Now Cloud computing has been concentrate on many recent research and implementation, which ensures reliable and secure transfer of files. In this paper we discussed about the survey on access controls Security issues in cloud computing. The existing solutions are role based access control, identification based access control, attribute based access control and hierarchical based access control. Still existing solution are not sufficient to trust the cloud. The future plan is to implement a trust model for secure storage of file.

REFERENCES

[1] Hongwei Li, Yuanshun Dai1, Ling Tian, "Identity based authentication for cloud computing", Springer-Verlag Berlin Heidelberg, pp 157-166, 2009.
[2] Cheng-Chi Lee1, Pei-Shan Chung2, and Min-Shiang Hwang "A Survey on Attribute-based Encryption Schemes of Access Control in Cloud Environments Attribute-based encryption", International Journal of Network Security, Vol.15, No.4, PP.231-240, July 2013.
[3] Junbeom Hur"Improving Security and Efficiency in Attribute-Based Data Sharing", IEEE Transactions on Knowledge And Data Engineering, Vol. 25, No 10, October 2013
[4] Ming Li, Shucheng Yu, Yao Zheng, Kui Ren, and Wenjing Lou, "Scalable and Secure Sharing of Personal Health Records in Cloud Computing using Attribute-based Encryption",IEEE Transactions on parallel and distributed systems, Vol 24,No 1,Jan 2013
[5] Liang Yan, Chunming Rong, and Gansen Zhao, "Strengthen Cloud Computing Security with Federal Identity Management Using Hierarchical Identity-Based Cryptography", © Springer-Verlag Berlin Heidelberg,pp167-177, 2009
[6] Changji Wang, Yang liu"A secure and Efficient Key-Policy attribute based Encryption Scheme",International Conference on information science and Engineering.2009
[7] Changji wang, Xuan Liu,Wentao Li,"Implementing a Personal Health Record Cloud Platform using Ciphertext-Policy Attribute Based Encryption",International Confercne on Intelleigent Networking and Collaborative Systems,2012.
[8] Frederic Nzanywayingoma,Qiming Huang,"Securable Personal Health Records using ciphertext Policy Attribute Based Encryption"International Conference on E-Health Netwoking,Apllications and Services",IEEE 14th International conference on e-health networking, applications and services, ISBN
978-1-4577-2039-0, pp 502-505,2012.
[9] Zhiguo Wan, Jun'e Liu, and Robert H. Deng,"HASBE: A Hierarchical attribute based solution for flexible and scalable access control in cloud computing", IEEE Transactions on Information Forensics and Security,Vol 7, No 2, April 2012.
[10] Deepthi Adulapuram," Hierarchical Attribute –Set-Based Encryption", IRACST – International Journal of Computer Science and Information Technology & Security (IJCSITS), ISSN: 2249-9555,Vol.3, No.4, August 2013
[11] U Jyothi, Nagi Reddy, B Ravi Prasad, "Review of "Achieving Secure, Scalable and Fine Grained data Access Control in Cloud Computing" International Journal Of Engineering And Computer Science ISSN:2319-7242,Volume 2 Issue 8 August, 2013 Page No.2440-2447
[12] Zhiguo Wan, Jun'e Liu, and Robert H. Deng,"HASBE: A Hierarchical Attribute Based Solution for Flexible and Scalbale Access Control in Cloud Computing" IEEE Transactions On Information Forensics and Security,Vol 7 , No 2, April 2012
[13] Kan Yang, Xiaohua Jia, Expressive, Efficient, and Revocable Data Access Control for Multi-Authority cloud Storage" IEEE Transactions on Parallel and Distributed Systems,Vol,25,No 7, July 2014.