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 9, September 2017

Survey on Authentications Issues in Cloud Computing

Vatsala Tamrakar[1], Prof. Rajendra Arakh[2], Prof. Sumit Nema[3]

M.Tech. Student, Department of Computer Science Engineering, Global Engineering College, Jabalpur, Madhya Pradesh, India[1]

Assistant Professor, Department of Computer Science Engineering, Global Engineering College, Jabalpur, Madhya Pradesh, India[2]

Assistant Professor and Head of The Department, Department of Computer Science Engineering, Global Engineering College, Jabalpur, Madhya Pradesh, India[3]

ABSTRACT: Cloud computing has been a hot researching area of computer network technology. Some giant companies can offer the cloud services now. With the development of cloud computing, a set of security problem appears, such as accessing security and so on. This paper surveys the security problems of current cloud computing. Then based on the architecture of cloud computing, a security model is proposed. 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 users' 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, 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 analyse 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.

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.

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 9, September 2017

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 are 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 cipher text-policy attributes based encryption.

D. Key-Policy based Encryption

In key-policy attribute-based encryption, Cipher text 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 cipher text.

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 labelled with set of attributes [6]. The drawback in KP-ABE scheme is that data owner doesn't 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 cipher text 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.E.g.: 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 9, September 2017

E. Cipher text policy based attributes based Encryption

In CP-ABE, the private key is associated with a set of attributes, and a cipher text are created with access structure, which is used to specify the encryption policy. A user can decrypt the cipher text 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 cipher text- 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 authority 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 untrusted 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.

G. Multiauthority

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 do 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.

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 9, September 2017

Table 1. Techniques and its Advantage & Disadvantage

S. No.	Technique Name	Observation	Advantage	Disdvantage
1.	Identity based encryption	Identity based system generates any party public key with their identity. Trusted third party generates the private key. The public key generator publishes the master public key and any party can compute the private key combining the master public key and identity policy with which user can decrypt the message. This technique is useful where pre distribution of authenticated secret key is infeasible and there is no need of distribution of keys between users.	• Reduces the complexity of the encryption Process. • No certificates needed. • No pre-enrolment required. • Keys expire, so they don't need to be revoked. In a traditional public-key system, keys must be revoked if compromised.	• A secure channel between User and private key generator is required. • PKG need high level of assurance, since it holds all Private keys and must remain online. •Encrypted data is decrypted only by one known user so this lacks advance data sharing.
2.	Attribute based encryption	The attribute authority generates public Key and master key according to attributes. The data owner encrypts the data with a public key and a set of descriptive attributes. Data users decrypt the encrypted data with his own private key sent from the authority, and then he can obtain the needed data.	• Reduce the communication overhead. • Provide a fine-grained access control. • Collusion-resistance is crucial security feature of Attribute-Based Encryption	The data owner needs to use each authorized user's public key to encrypt data.
3.	KP-ABE	Files are encrypted and loaded using some attribute and users with all those attribute only be able to decrypt. In KP-ABE system, ciphertext are associated with a set of descriptive attributes, while trusted attribute authority issues private key to user which captures an policy that Specifies which type of ciphertexts the key can decrypt.	• Its designed for one-to-many communications. • Achieve fine-grained access control. • More flexible to control users than ABE scheme.	The data owner cannot decide who can decrypt the encrypted data. It's not suitable for some application because data owner has to trust the key issuer[14].
4.	CP-ABE	Ciphertext policy is the access structure on ciphertext. By using this technique even if the storage server is untrusted data can be made confidential. In a ciphertext-policy attribute-based encryption (CP-ABE) system, when a data owner encrypts a message, which specify a specific access policy in the ciphertext, stating who can decrypt the encrypted data.	The disadvantage of KP-ABE is over come in CP-ABE and it support the access control in the real environment.	The user combine all attributes in a single set issued in their keys to satisfy policies.
5.	Role based	The data owner encrypts the datas in cloud with particular encryption policy and grant access to the users with particular specific roles. There are specific set of roles and to which the users are assigned and each role has set of assigned permission.	This technique reports savings from more efficient provisioning, more efficient access control policy administration and reduced employee down time. ABE are easy to set up and complex to manage this is over come by Role based encryption technique.	An efficient cryptographical method to validate the partial ordering relation among these keys are required.
6.	Hierarchical Attribute-set-based encryption	Data owner encrypt the data and send the encrypted data to the cloud. The policy of the data files can be changed by the owner by updating the expiration time. Domain authority provides with the privileges and data owners are	• Less initial capital investment • Shorter start-up time for new services • Lower maintenance cost and operation costs	

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 9, September 2017

		controlled by domain authority.	• Easier disaster recovery.	
7.	Multi authority	This technique generates centralised private key for the user, centralised secret key. The system is built up of a Central Authority (CA) and multiple attribute authorities (AAs).These attribute authorities separately maintain attributes. The major components of the scheme are master attribute authorities and users. The duty of the master is to distribute private user keys. Attribute Authority certifies the user and distributes private attribute key to the user that can be used for decrypting the ciphertext. User produces ciphertext by the method of encryption technique.	Different attribute domains are managed by different authorities. • Expressiveness, efficiency and security are not weaker than that of the single-authority. • No authority can independently decrypt any ciphertext. • The advantage of the system is that the system provides collusion resistance; the system is more efficient, more robust and provides scalability. • The authorities are working independently of each other. • Therefore, the failure or malfunctioning of one authority will not affect the working of other authorities. This improves the robustness of the system.	The CA can decrypt every ciphertext so that the user privacy and confidentiality of the data is less in this system. •There is overhead involved in managing the distributed authorities.

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 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.