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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2016

A Survey on Secure Data Sharing Methods in Cloud Storage

Mohis M[1], Devi Priya V S[2]

M.Tech Student, Department of Computer Engineering, Mar Baselios College of Engineering and Technology, Nalanchira, Trivandrum, India[1]

Assistant Professor, Department of Computer Engineering, Mar Baselios College of Engineering and Technology, Nalanchira, Trivandrum, India[2]

ABSTRACT: Cloud computing provides elastic, flexible and on demand storage and also provides computing services to customers. Many of the organizations choose the cloud platform for data sharing and processing. It liberates organizations from in-house data storage systems. Cloud provides pay per usage model and thereby organizations with low budget can utilize high computing and storage services with low cost. In today's IT industry cloud computing helps to access on demand network and a shared pool of resources that are made available to their own requirements. Cloud storage allows data owners to store and share data and also provides efficient data management for freeing the wastage of space. Sometimes data owners may lose confidentiality and security over the shared data. Many of the encryption techniques are used for addressing the security issues inside cloud. Attribute based and other hierarchical based methods are the most widely used techniques for providing data confidentiality and access control to data stored in cloud where most of the traditional encryption schemes failed to address. A brief survey of methods that are used for sharing data through cloud is covered with their own advantages and disadvantages.

KEYWORDS: Cloud computing, Attribute Based Encryption (ABE), Proxy Re- Encryption, Mediated Certificateless encryption, Security issues, Confidentiality.

I. INTRODUCTION

Cloud computing[10] is a model for accessing a shared pool that enables ubiquitous network access and computing resources that are configurable. Processing and storing cloud computing and storage solutions provide various capabilities to third-party data centres. Similar to utility models such as electricity grid cloud computing relies the sharing of resources for achieving economies of scale. Cloud concept is the foundation for broader concept of converged infrastructure. Cloud systems can be used to provide capabilities such as data sharing to organizations and provides more benefits. [10]

Different users from various organizations passing data in the cloud, data uploading time and cost of data must be correlated for exchanging data manually. To making renitent and obsolete document, cloud creates clusters inside the storage. Social networking sites like facebook, twitter sharing media like photos and videos are made easy through cloud sharing. For students and group related activities there is major importance for group tools for data storing and efficient data management. There arises the need for sharing information to group of people. Cloud enables and provides platform for group management data sharing methods. Since there are many privacy issues related to cloud computing many users can access the critical data that are shared by other users.[11]

Public cloud[10] provides service over a network for public use and it is open for all users. Public cloud services use pay per usage model and may be free. In case of public and private cloud there is no difference in architecture but security considerations may be different for both such as applications storage and other resources. These services are made available for public users and audience communication may be affected to the non-trusted network.

Data sharing in cloud must be secure and achieves confidentiality to the data. An efficient method recently used for sharing sensitive data in cloud is mediated certificateless encryption which offers more security. Because of the pairing less operations, this method enables immediate revocation thereby ensures security and confidentiality to the data which resides in the cloud. Existing problems such as key escrow and certificate revocation problem can be overcome

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2016

by this approach. Using this method, in the data owner module, overall overhead can be avoided and single encryption is carried out in the whole process.

II. RELATED WORK

Cloud computing enables and provides a new world of opportunities for business. There is numerous security challenges that need to be considered and addressed to protect and secure the cloud computing strategy .There are many different encryption schemes that have been proposed to address the security issues for data sharing inside cloud. Some of them are discussed below.

A. Attribute Based Data Sharing Scheme

Yu, Shucheng, Cong Wang, Kui Ren, and Wenjing Lou[1] proposed a method of encryption which is Cipher text-Policy Attribute Based Encryption (CP-ABE) provides fine-grained access control. Each user is associated with a set of attributes and encryption is taking place with access structures on attributes. In the case of cipher text decryption the attribute must satisfy the cipher text access structure.. Therefore a security model was found effective that protects the possible attacks to sensitive data and enables revocation of attribute of data at any time [1].

Fig.1 shows method of data sharing. One of the major problem faced during data sharing is revocation of attributes, It can be solved using this method for limited instances..In this method of cryptography there is a master key component which defines the public key and secret key for the user. Each of these keys belongs to users attributes. [1]

This method efficiently handles the attribute revocation problems in case of attribute based systems. This can be implemented in case of semi trustable proxy servers for supporting attribute revocation. This scheme places minimal load on authority upon these revocation events. By combining the proxy re-encryption with CP-ABE this technique is secure against the chosen plain text attacks. [1]

The main drawback of this scheme is that it doesn't avoid the key escrow problem and also the Proxy servers have no provision to update secret key without revealing the attribute information.

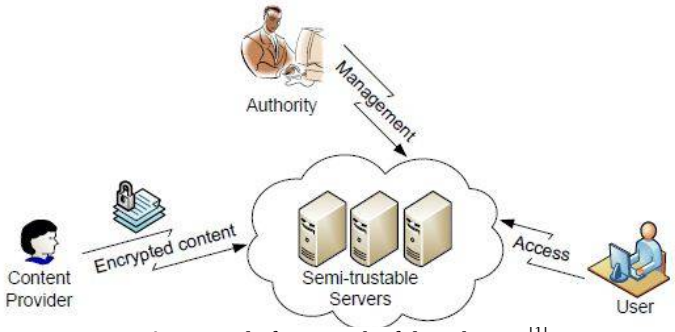

Fig. 1. An example framework of data sharing [1]

B. Content Dissemination for Privacy preserving in cloud

Shang, Ning, Mohamed Nabeel, Federica Paci, and Elisa Bertino[2] proposed a Privacy preserving scheme which is a group key management scheme. This method is used in the case of selective distribution of contents or documents which are encoded which preserves where the document is delivered. It is a broadcasting approach based on the access control policies of users whom can access documents or sub documents. Each broadcast document is segmented into different -different sub documents based on the access control policies and encrypted with different key. In this method users with identity attributes will get the policies and is based on modern attribute-based access control and the policies are privileged to the user's identity [2]. According to access control policies here users are granted access to each documents and sub documents about their document publisher's identity attributes. In this method document publisher doesn't learn not only the users with identity attributes but also policy conditions are verified by the users. Thereby the inferences about the values of identity attributes can be prevented. In this system there is no need to send encrypted

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2016

document and decryption keys. On basis of subscription information users gain the privacy to reconstruct the keys to decrypt authorized persons. New subscription and revocation of subscriptions also handles in this scheme [2].

The main disadvantage of this method is instead of it enables Privacy protection to users and creates transparent rekey to users but it doesn't supports expressive access control policies and clustering subscribers is not supported.

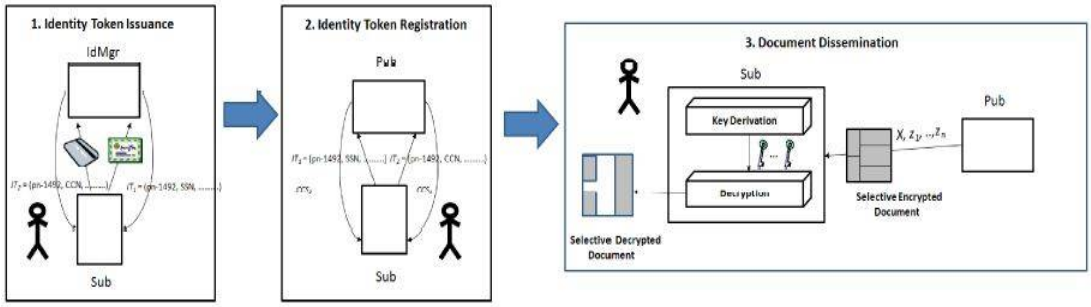

Fig. 2. Overview of Content Dissemination scheme [2]

C. *Fine-Grained access control based sharing in public clouds*

Nabeel, Mohamed, and Elisa Bertino[3] explained that ,While data sharing is carried out in public clouds mostly the problem experienced is that how the selection of shared data which is based on fine-grained and attribute based access control policies are carried out and also assures confidentiality and privacy preserving of users from cloud. In this case to address the issues of data confidentiality encryption is the commonly adopted method for assuring data confidentiality. Along with encryption organizations that enforces fine grained access to data. This Control access is based on identity attributes like security relevant properties. Access control systems in this method is commonly referred to as attribute based access control (ABAC).An approach to support fine-grained selective ABAC is to identify the sets and the encryption of each set is carried out with the same encryption key. According to the access control policies each user give the key to the sets after uploading the data to the cloud. This method addresses the main issues such as data protection and assures confidentiality from the cloud. This enforces fine-grained access control policies with respect to the users whom request the data from cloud. Key management is the major issue in this approach that is with respect to the access control policies each user must be given the actual keys to the users [3].

This scheme has some disadvantages such as Identity attributes cannot be efficiently handling in this method for adding and revoking users and also the policy changes cannot be carried out properly. Here requires different keys which are encrypted copies. It needs high computational costs and also revocation is supported by the help of additional attributes.

D. *HABSE : A Hierarchical attribute-based sharing in cloud*

Wan, Zhiguo, Jun E. Liu, and Robert H. Deng[4] implemented that ,In cloud computing, there are many schemes that are in relation with attribute-based encryption (ABE) had implemented for ensuring access control of data associated with cloud. But there is the problem that most methods are suffered for implementing complex access control policies to users and data. A method to realize flexible, scalable and fine-grained access control to the data in cloud is hierarchical attribute-set-based encryption (HASBE).This method is an extension of cipher text-policy attribute-set-based encryption (ASBE) and the user structure is in hierarchical manner. Because of the hierarchical structure this scheme achieves scalability as well as inherits flexibility and also supports fine-grained access by using compound attributes of cipher text-policy attribute-set-based encryption. For multiple value assignments hierarchical attribute-set-based encryption does multiple value assignments to perform access expiration time and thereby solves the user revocation [4].

Fig. 3 shows the entities in this scheme. The framework consists of five entities such as a cloud service provider, data owner, data consumers, a number of domain authorities, a trusted authority. Providing data storage services to cloud are managed by cloud service providers. Encryption is taken place by the data owner and stores it back to the cloud. To get access on the shared data encrypted files have been downloaded by the consumers. These data owners are

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2016

under the control of a domain authority, the overall control goes to the parent domain authority. This makes the hierarchical structure.[4]

Disadvantages includes this method contains all attributes are in same conjunctive clause therefore its not suitable to implement. The entire system is administrated by the same do-main authority or by multiple domain authorities. Decryption Keys in the hierarchical structure is disclosing to all users. Because of the hierarchical data sharing there arises the problem of heavy computation at the data owner part. [4]

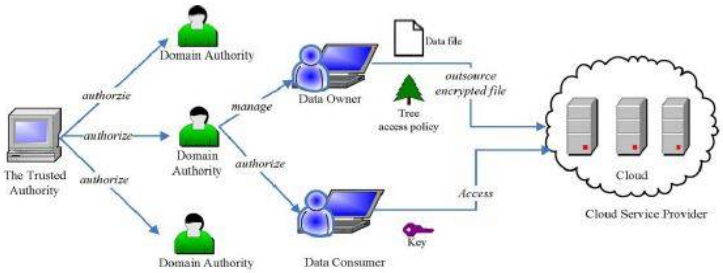

Fig. 3. Overview of HASBE scheme[4]

E. DFA based Proxy re-encryption scheme in cloud

Liang and Kaitai[6] proposed a DFA based encryption scheme in cloud, In this method a Proxy Re-Encryption (PRE), is also known as Deterministic Finite Automata Based Functional PRE (DFA-based FPRE)[6].DFA-based FPRE system adapts a new technique. Each message is associated with a arbitrary length string with index and the cipher text is associated with it. Decryption is carried out if and only if DFA is associated with his/her secret key which accepts the string. Re-encryption key is given by the semi-trusted proxy. This encryption is allowed to be transformed to another cipher text which is associated with new string in the semi-trusted proxy. The proxy cannot gain access to the associated plaintext. Flexibility can be increased by these new primitives and can delegate their decryption rights to other users. This method allows encryption which is associated with an arbitrary length index string. The plaintext can be recovered using the secret key associated with it. This operation is carried out if and only if Key accepts the string which is tagged by the DFA. Without disclosing the useful information to the proxy encryption will be carried out with the new index string associated with it. Other ways it permits a semi trusted proxy to transform an encryption associated with it. [6]

There exists a drawback that there is a weaker re-encryption scheme since proxy possesses keys of both parties simultaneously. When decryption of plain text takes place encryption takes place in the other side. But proxy re-encryption schemes are used for hiding either keys of a key of any party. Therefore it is not an ideal method for secure encryption.

F. Group sharing framework in cloud storage

In this scheme, an effective and secure group sharing framework for protecting data inside the public cloud that ensures protection against the attackers or third party servers. This technique includes proxy signature scheme, proxy re-encryption and enhanced group data sharing that together forms a protocol. Based on the proxy signature scheme group members get access from the group leader and group leader can effectively manage one or more group members same time. Even if all group members are not online this enhance TGDH scheme can negotiate and group key updating can take place with cloud servers. With the help of proxy re-encryption most of the operations which are computationally intensive will be delegated without revealing any secret information to the cloud. This scheme supports group key updating while joining and leaving of group members taking place. Without leaking the privacy of users this method helps to transmit most of the computational complexity and communication overhead. For any specific member he/she can get the group management privilege and that can be revoked at any time. In this enhanced group sharing even though group members are not online, offline members also can perform group synchronization when the user become online again. Because of the Group sharing framework there arises the problem of certificate

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2016

revocation [7].

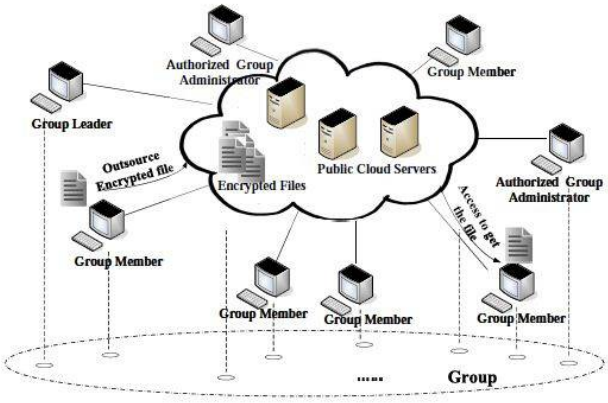

Fig. 4. An example for cloud based group sharing scenario [7]

G. *Security Mediated Certificateless Cryptography*

Security-mediated certificateless (SMC) cryptography is a version of mediated cryptography which is a lightweight scheme which is applicable to maintain the revocation of keys and instantaneous revocation. This technique can moreover solve the key escrow problem in comparing with the existing encryption algorithms. This technique efficiently handles fully-adaptive chosen cipher text attacker where the security method fails to handle. In this technique the algorithm is based on the bilinear pairing of operations. Other than the identity based encryption schemes this technique supports distributed security mediators.[5]

There are some disadvantages such as Expensive pairing operations in Mediated Certificateless-PKE schemes are either inefficient or vulnerable against partial decryption attacks. In the case of large re-encrypted data set each time the data owner needs to download the data for decryption and perform re-encryption with new keys since the data owner have no copies of data, this makes it inefficient. A private communication channel needs to be establishing for issue new keys to the users. It is not convenient for all time. [5]

H. *Mediated Certificateless encryption without Pairing*

While enforcing the access control mechanisms this method ensures confidentiality of sensitive data and other contents inside cloud. In this scheme there are mainly five entities that are user, data owner, Key Generation Centre (KGC), Security Mediator (SEM) and a storage service.[12]

The entities which reside in public cloud such as SEM, KGC and the encrypted storage are semi-trusted. Because of the confidentiality of keys and data elements inside the cloud they are not fully trusted. But it is trusted for correct execution of protocols. By using symmetric encryption algorithm that encrypts the data items and in mCL-PKE scheme because of access control policy symmetric encryption is carried out by data owner resulting the encrypted data items and the encryption key will be uploaded to the cloud. The most efficient advantage in this scheme is the presence of KGC in the cloud i.e., the key Generation Centre which is the only entity which have rights to generate the keys and it differentiates this method for the conventional approaches. These approaches help to manage keys for each organization. In normal Certificateless-Public Key Encryption method Key generated by the user is completely secure and secret and the private key which is generated by the Key Generation Centre.[12]Improved method includes a security mediator which accepts the key values such as partial private key, secret key value and the user's private key generated in the mediated encryption scheme. Access request is given by the security mediator based on the request sent by the user. User sends request each time whenever they want to get data. Partial decryption and revocation is checked by these security mediators. Key escrow problem can hold off since the private key of user is never acknowledged to any of the external sources. Revocation problem can be solved because key generation centre and security mediator doesn't send access request for a named person. These are the main advantages of the scheme.[12]

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2016

III. DISCUSSION

Different attribute based and proxy re encryption schemes addresses security issues associated with sensitive data in cloud.

Table1 shows comparison over different methods that are used to share data in cloud,

Table 1. Comparison of different attribute encryption [9]

Techniques/Parameter	Attribute Based Encryption	Content Dissemination	Proxy re-encryption	Hash Based Scheme	Mediated Certificateless Encryption
Fine grained Access Control	Low	Low, High if there is re-encryption technique	Average Realization of Complex Access Control	Good Access control	Excellent access control
Efficiency	Average	Average, High for broadcast type system	Average, Not efficient for modern enterprise environments	Flexible	Flexible
Computational Overhead	High	Most of computational overheads	Average computational overheads	Some of overhead	No overhead
Collision resistant	Average	good	good	good	Better than others

IV. CONCLUSION

In the near future Cloud data sharing is fast becoming available than other traditional data sharing methods. Different encryptions such as ABE and PRE addresses the security issues related to sensitive data inside the cloud. The recently implemented technique that is mediated Certificateless Public Key Encryption scheme is carried out without pairing operations provides formal security for sensitive and private data inside cloud. This scheme mainly addresses the issues of key escrow problem and certificate revocation. By implementing the mCL-PKE scheme as a secure and efficient method, which is an improved approach to securely share sensitive data which is stored inside public clouds. Immediate revocation and confidentiality is ensures by this scheme. Then for additional security recently proposes to embed the cipher text inside a noise such as text or audio and upload to the cloud. There by when an attacker enter into cloud and try to modify the content, the actual content is not visible to him, only noise will be visible to the attacker.

ACKNOWLEDGEMENT

We would like to thank my guide and other faculty members of Mar Baselios College of engineering and technology, who provided their helping hands in the successful completion of this survey.

REFERENCES

1. Yu, Shucheng, Cong Wang, Kui Ren, and Wenjing Lou. “Attribute based data sharing with attribute revocation.“InProceedings of the 5th ACM Symposium on Information, Computer and Communications Security, pp. 261-270. ACM, 2010.
2. Shang, Ning, Mohamed Nabeel, Federica Paci, and Elisa Bertino.“A privacy-preserving approach to policy-based content dissemination.“ In-Data Engineering (ICDE), 2010 IEEE 26th International Conference on, pp. 944-955. IEEE, 2010.
3. Nabeel, Mohamed, and Elisa Bertino. “Privacy-Preserving Fine-Grained Access Control in Public Clouds.“IEEE Data Eng. Bull.35, no. 4 (2012): 21-30.
4. Wan, Zhiguo, Jun E. Liu, and Robert H. Deng. “HASBE: a hierarchical attribute-based solution for flexible and scalable access control in cloud computing.“ Information Forensics and Security, IEEE Transactions on7.2 (2012): 743-754.
5. Chow, Sherman SM, Colin Boyd, and Juan Manuel Gonzlez Nieto.“Security-mediated certificateless cryptography.“Public Key Cryptography-PKC 2006. Springer Berlin Heidelberg, 2013. 508-524.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2016

6. Liang, Kaitai, et al."A DFA-based functional proxy re-encryption scheme for secure public cloud data sharing."Information Forensics and Security, IEEE Transactions on9.10 (2014): 1667-1680.
7. Xue, Kaiping, and Peilin Hong."A Dynamic Secure Group Sharing Framework in Public Cloud Computing."Cloud Computing, IEEE Transactions on2.4 (2014): 459-470.
8. Nabeel, Mohamed, and Elisa Bertino."Privacy Preserving Delegated access control in Public clouds." Knowledge and Data Engineering, IEEE Transactions on26.9 (2014): 2268-2280.
9. Minu George, Dr. C.Suresh Gnanadhas, Saranya.K."A Survey on At-tribute Based Encryption Scheme in Cloud Computing."International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 11, November 2013.
10. https://en.wikipedia.org/wiki/Cloud_computing
11. Zhang, Q., Cheng, L., & Boutaba, R. (2010). Cloud computing: state-of-the-art and research challenges. *Journal of internet services and applications*,*1*(1), 7-18.
12. Seo, S. H., Nabeel, M., Ding, X., & Bertino, E. (2014). An efficient certificateless encryption for secure data sharing in public clouds. *IEEE Transactions on Knowledge and Data Engineering*, *26*(9), 2107-2119.