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. 3, Issue 10, October 2015

Survey on Secure Data Sharing using Encryption Techniques

S. Sathya[1], Dr. B. Vanathi[2]

Student II Year M.E, Dept. of CSE, Valliammai Engineering College, Chennai, India [1]

Professor , Dept. of CSE, Valliammai Engineering College, Chennai, India [2]

ABSTRACT: A cloud computing is mainly used for storing a huge amount of data on cloud serverandit gives On Demand access to a common pool of resources in the cloud server. Sharing of data on cloud server and giving data security and privacy is a basic issue in the cloud server.In order to make data to be secure, it is necessary to implement any efficient and secure data access control method. As the data is shared over the network, the data ought to be encrypted to keep up privacy against untrusted users. There are different encryption schemes that provide security and access control over the network. In this paper, literatures on data encryption techniques like ABE, KP-ABE,CP-ABE, PRE, CPREare discussed.

KEYWORDS: ABE, PRE, Access control.

I. INTRODUCTION

Cloud Computing is a distributed computing paradigm where the computing resource such as hardware, software, processing power are delivered as network services. The cloud computing model allows the user to access information and computer resource from anywhere in the internet connection available. To the users, cloud computing is a Pay-per-Use On-Demand mode that can easily access shared IT resources through the Internet.

A Cloud Computing mainly focuses onthe enterprise application environment. It is used for large amount data access in the cloud server. The Cloud has the capability to achieve the large amount of data quickly and easily for the client.
Cloud storage is a flexible method for access of data anytime secure manner. For protecting theconfidentiality of the stored data, the data must be encrypted before uploading to the cloud by using some cryptographic methods.Characteristics of secure cloud data storage are Integrity, Availability and Confidentiality. The Advantages of cloud storage over traditional server are

- Flexible data access,
- Secure data storage,
- High availability,
- Enhanced sharing.

Some examples of enterprise services of cloud computing:

- Google
- Amazon
- Salesforces.com etc..

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. 3, Issue 10, October 2015

II. LITERATURE SURVEY

Different Encryption methods are discussed below:

1. ATTRIBUTE BASED ENCRYPTION (ABE)

Attribute Based Encryption (ABE)method introduced by Sahai and Waters in the year 2005 and the main objective is to provide data security. In this ABE scheme, there are three types of entities, Third party, Admin (Data Owner, Sender) and Data User (Receiver).The third party makes the keys based on the user attributes. Here the secret key of the user and the cipher text are depend on the attributes.

Data Owner's generallyuse two operations: Data Sharing and Data Searching. The role of the Admin is to encrypt the data with a public key and a set of descriptive attributes. The Data User's part is to decrypt the encrypted data based on the attributes and with the private key. The decryption is conceivable just if the set of attributes of the user key matches the attributes of the cipher text.

For Examples: (Chair, Food, Lion, Scooter)

ADVANTAGES
ABE scheme has significant advantages ofa flexible one to many encryption usage.
DISADVANTAGES
Attribute based encryption (ABE) scheme is that the data owner needs to use every authorized user's public key to encrypt data.

2. KEY POLICY ATTRIBUTE BASED ENCRYPTION (KP-ABE)

V. Goyal, et al. [1]Proposed a key-policy attribute-based encryption (KP-ABE) scheme. It was introduced to conquer the impediments of ABE scheme.In this schema, it uses a set of attributes to detail the encrypted data and it forms the access policies in the user's private key. If the attributes of the encrypted data can fulfill the access structure in user's private key,then the user can derive the message content through any decryption algorithm.Key Policy Attribute Based Encryption (KP-ABE) method, a public key encryption strategy that is expected for one-to-numerous correspondences.This scheme enables a data owner to diminish by far most of the computational overhead to cloud servers. KP-ABE method used for encryption toprovide fine-grained access controlEvery record or message is encrypted with a symmetric data encryption key (DEK), which is over again encrypted by a public key relating to a set of attributes in a set of attributes in KPABE, which is produced compared to an access structure.The data file that is encrypted is put away with the comparing attributes and the encrypted DEK.Just if the corresponding attributes of a record or messages stored in the cloud satisfy the access structure of a user's key, then the user is ready to decrypt the encrypted data encryption key, which is used to decrypt the file or message.

ADVANTAGES:
Fine grained access,
Reduce the computational overhead,
Data confidentiality,
In this method mainly used for a secure forensic analysis purpose.

DISADVANTAGES:

The main disadvantagekey-policy attribute-based encryption, the data owner is also a Trusted Authority (TA) at the same time.

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. 3, Issue 10, October 2015

3. CIPHER TEXT POLICY ATTRIBUTE BASED ENCRYPTION (CP-ABE)

Sahai[2] proposed by the CP-ABE scheme. CP-ABE method, every ciphertext is relatedto an access policy on attributes and every user's private key is relatedto a set of attributes.A user has the capacity decrypts a ciphertext just if the arrangement of attributes connected with the user's private key fulfills the access policy connected with the ciphertext.CP-ABE works in the inverse process of KP-ABE scheme. The access structure of this scheme or algorithm, it acquires the same technique which wasutilized as part of the KP-ABE to build and the access structure built into the encrypted data can let the encrypted data choose which key can improve the data; it means the user's key with the attributes just satisfies the access structure of the encrypted data. Furthermore, the concept of this plan is like the conventional access control schemes.The Encryptor who indicates the limit access structure for his intrigued attributes while encrypting a message. In view of this access structure message is then encrypted such that just those whose attributes fulfill the access structure can decrypt it.

ADVANTAGES:
Fine grained access.
Data confidentiality.

DISADVANTAGES:
Not fulfilling enterprise environment access control,
Limitation of specifying policies and managing user attributes.

4. PROXY RE ENCRYPTION(PRE)

Proxy Re-Encryption (PRE) [3] framework is to safely empower the re-encryption of cipher texts starting with one key,then onto the next, without depending on trusted parties. A Proxy can change without seeing the Plaintext cipher text encrypted under one key into an encryption of the same plaintext under another key.Proxy Re-Encryption is a type of public key encryption that permits a user Alice to "delegate" her decryption rights to another user Bob.In a PRE Scheme, a proxy gives a bit of data that permits turning a cipher text encrypted under a given public key into an encryption of the same message under an alternate key.

Guaranteeing the security and protection of data stored on outside cloud storage services is of essential significance to authoritative and individual users, and one ordinary method for accomplishing this is utilizing encryption (by the data owner).

PRE schemes can be classified into two categories according to the direction of delegation:

- Bi directional Proxy Re encryption Function (BPF)
- Unidirectional Proxy Re Encryption Function (UPF)

Bi directional Proxy Re encryption Function (BPF)

The re-encryption key can be utilized to make the re-encryption in both directions, the PRE scheme is called bidirectional Proxy Re encryption Function (BPF) as shown in Figure 1.

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. 3, Issue 10, October 2015

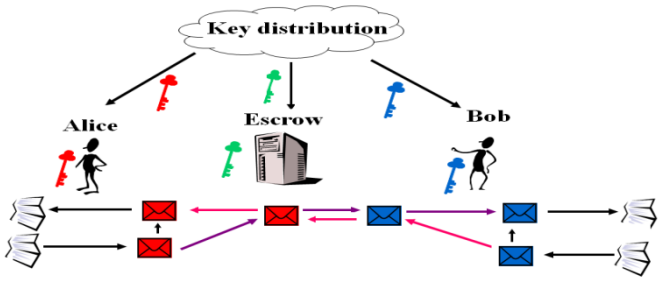

Figure.1 Bi Directional Proxy Re Encryption Function

Unidirectional Proxy Re Encryption Function(UPF)

The re-encryption key doesn't used to the re-encryption in both directions, the PRE scheme is called Unidirectional Proxy Re encryption Function(UPF) as shown in figure 2

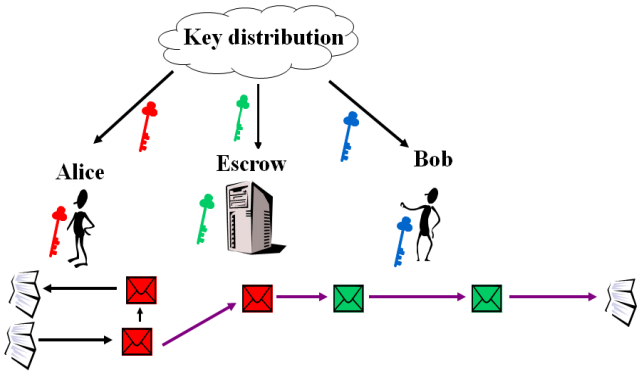

Figure.2 Unidirectional Proxy Re Encryption Function

5. CONDITIONAL PROXY RE ENCRYPTION(C-PRE)

The C-PRE [4] scheme involves three principles: a delegator (Ui), a proxy and a delegate (Uj). A message sent to delegator Uiusing condition w is encrypted by the sender using both Ui's public key and condition's. To re-encrypt the message to Uj the proxy is given the re-encryption key (rki→ j) and the condition key (cki, w) corresponding to w. Both the keys can be generated only by ui. These two keys from the secret trapdoor used by the proxy to perform ciphertext translation. The proxy is not capable to translate those ciphertext whose corresponding condition keys are not available. Therefore, Ui has a flexible control on delegation by letting go condition keys properly.

ADVANTAGES:

Fine Grained Access
High scalability
Data Confidentiality
Unidirectional.

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. 3, Issue 10, October 2015

DISADVANTAGES:

Anonymous given the condition for security against the method.

The Different ABE techniques are Table 1: Comparison of ABE schemes

Technique	Fine grained access control	Efficiency	Computational Overhead	Collision resistant
ABE	Low	Average	High	Average
KP-ABE	Low	Average	Most are computation al overhead	Good
CP-ABE	Average	Average	Average	Good

The Different PRE techniques are Table 2: Comparison of PRE schemes

Technique	Data Encryption	Finegrained access Control	ROM	Collision resistant
PRE	Yes	Good	Yes	Average
C-PRE	Yes	Average	Yes	Good

III. CONCLUSION

In this paper, several encryption schemes for secure sharing of data in cloud. Many encryption schemes like ABE, KP-ABE, PRE, and C-PRE are discussed in which all the schemes are resilient in efficient access control.Based on the discussion data's are encrypted and need to maintenance for a number of users. Each method (scheme) has a public key, secret key and random polynomial. Authorized can access to decrypt the cloud data. These papers conclude a survey based on ABE and PRE schemes that provide security and performance level.

REFERENCES

1. V. Goyal, O. Pandey, A. Sahai, and B.Waters "Attribute-based encryption for fine-grained access control of encrypted data," in Proceedings of the 13th ACM conference on Computer and communications security, pp. 89{98, 2006}
2. J. Bettencourt, A. Sahai, and B.Waters "Ciphertext-Policy Attribute Based Encryption "in Proceedings of IEEE Symposium on Security and Privacy, pp 321V334, 2007.

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. 3, Issue 10, October 2015

3. G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage", ACM Trans. Information and System Security, 2006, pp. 1-30.
4. JianWeng, Robert H. Deng, Xuhua Ding, Cheng-Kang Chu, and Junzuo Lai, " Conditional proxy reencryption secure against chosen-ciphertext attack", In ASIACCS,2009,pp. 322−332.
5. Changji Wang and JianfaLuo," An Efficient Key-Policy Attribute-Based Encryption Scheme with Constant Ciphertext Length", Hindawi Publishing Corporation Mathematical Problems in Engineering, Volume 2013, Article ID 810969, 7 pages
6. Jun Shao, Rongxing Lu, Xiaodong Lin, KaitaiLiang , "Secure bidirectional proxy re-encryption for cryptographic cloud storage", Pervasive and Mobile Computing(2015).