RESEARCH ARTICLE OPEN ACCESS

A Survey on Secure Data Accessing and Sharing Using Cryptographic Algorithms in Cloud Computing Environment

J. Mala*, Dr.A.N. Jayanthi**, S. Rajesh***

*(Information Technology, Sri Ramakrishna Institute of Technology, Coimbatore)

**(Electronics and Communication Engineering, Sri Ramakrishna Institute of Technology, Coimbatore)

***(Computer Science and Engineering, Sri Ramakrishna Institute of Technology, Coimbatore)

Abstract

Data sharing in the cloud is a method that allows users to conveniently access data over the cloud. The data owner outsources their data in the cloud due to cost reduction and the great accessibilities provided by cloud services. Data owner is not able to control over their data, because cloud service provider is a third party user. The major problem with data sharing and accessing in the cloud is the privacy and security issues. Various Cryptographic techniques are available to maintain user privacy and secure data sharing. This paper is mainly focus on several encryption methods to deal with secure data sharing and accessing in the cloud computing environment.

Keywords **-** Cloud, data sharing, access control, security, privacy, encryption

I. INTRODUCTION

Cloud computing can be used to enable data sharing capabilities and this can provide several benefits to the user and organization when the data shared in cloud. Since many users can contribute their data to the Cloud, the time and cost will be less compared to manually exchange of data.Persons love to share their information with others such as family, colleagues, friends or the world. Scholars also get benefit when working on team projects, as they are able to team up with members and get work done efficiently. This allows higher productivity compared to previous methods of frequently sending updated versions of a document to members of the group via email attachments.

II. SECURITY REQUIREMENTS

The security requirements for data sharing in cloud computing system are as follows:

1. **Data security**

   The provider must ensure that their data outsourced to the cloud is secure and the provider has to take security measures to protect their information in cloud.

2. **Privacy**

   The provider must ensure that all critical data are encrypted and that only authorized users have access to data in its entirety.

3. **Data confidentiality**

   The cloud users want to make sure that their data contents are not made available to unauthorised users. Only authorized users can access the sensitive data while others should not access any information of the data in cloud.

4. **Fine-grained access control**

   Data owner can restrict the unauthorized users to access the data outsource to cloud. The data owner grants different access rights to a set of user to access the data, while others not allowed to access without permissions. The access permission should be controlled only by the owner in un-trusted cloud environments.

5. **User revocation**

   When a user gets back the access rights to the data, it will not allow any other user to access the data at the given time. The user revocation must not affect the other authorised users in the group.

6. **Scalability**

   The number of users is extremely large in cloud. Also the users join and leave unpredictably from the cloud, it is important that the system maintain efficiency as well as scalability.

III. LITERATURE SURVEY

Some of the encryption techniques are discussed and summarized as follows.

A. Attribute Based Encryption (ABE):

Saravana Kumar Na et.al [3] proposed an Attribute Based Encryption(ABE) scheme. Encryption means conversion of original data into human unreadable form. Decryption means conversion of the encoded form into original form. By encrypting the data, the authorized person only can decode the original data. Thus data confidentiality is achieved by the encryption. There are many encryption algorithms today and has its many

advantages. The attribute based encryption is a verified algorithm for cloud computing environment. The restrictions of some of attribute based encryption method are to be analysed. Encryption in attribute based encryption is easy, secure and inexpensive compared to other encryption algorithm. The ABE is secure because the encrypted data contains the attributes rather than the data The limitation of the attribute based encryption is decryption of data is expensive [2]. The attribute based encryption makes the application to be secure the performance of the ABE is high compared to other encryption methods. Thus attribute based encryption is the solution to all cloud applications in future. The cloud is moved to next generation computing with critical applications and real time applications.

B. Key Policy Attribute Based Encryption(KP-ABE):

A. Sahai, and B. Waters et.al [5] proposed a key-policy attribute-based encryption (KP-ABE) scheme. It is the revised form of usual model of ABE. In KP-ABE technique, attribute policies are associated with keys and data is associated with attributes. The keys are associated with the policy which is to be satisfied by the attributes that are associating the decrypted data. Key Policy Attribute Based Encryption (KP-ABE) scheme is a public key encryption technique that is considered for one-to-many communications. Here, the data is associated with the attributes for which a public key is defined for each data. Encryptor, that is who encrypts the data, is associated with the set of attributes to the data or message by encrypting it with a public key. Users are allotted with an access tree structure over the data attributes. The nodes and structure of the access tree are threshold entries. The leaf nodes are associated with attributes. The user secret key is defined to reflect the access tree structure. Hence, the user is able to decrypt the message that is a cipher text if and only if the data attributes satisfy the access tree structure. In KP-ABE, a set of attributes is associated with cipher text and the user's decryption key is associated with a monotonic access tree structure [6].

When the attributes associated with the cipher text satisfy the access tree structure, then the user can decrypt the cipher text. In cloud computing, an efficient revocation and an access control mechanism on KP-ABE and a re-encryption techniques are used together. It enables a data owner to reduce the server computational overhead. The KP-ABE scheme provides fine-grained access control. Each message is encrypted with a symmetric data encryption key, which is yet again encrypted by a public key, that is corresponding to a set of attributes in KP-ABE, which is created corresponding to an access tree structure. The encrypted data files are stored with the corresponding attributes and the encrypted DEK. If and only if the corresponding attributes of a files are stored in the cloud fulfil the access structure of a user's key, then the user is able to decrypt the encrypted data encryption key [5].

That can be used to decrypt the file or message. KP-ABE scheme consists of the following four algorithms:

1. Setup: This algorithm takes as input a security parameter κ and returns the public key PK and a system master secret key MSK.PK is used by message senders for encryption. SK is used to generate user secret keys and is known only to the authority.

2. Encryption: This algorithm takes a message M, the public key PK, and a set of attributes as input. It outputs the cipher text E.

3. Key Generation: This algorithm takes as input an access structure T and the master secret key MSK. It outputs a secret key SK1 that enables the user to decrypt a message encrypted under a set of attributes if and only if matches T.

4. Decryption: It takes as input the user's secret key SK1 for access structure T and the cipher text E, which was encrypted under the attribute set. This algorithm outputs the message M if and only if the attribute set satisfies the user's access structure T.

C. Identity-Based Encryption (IBE):

Xinyi Huang et.al [7] proposed an Identity-based (ID-based) ring signature, which eliminates the process of certificate verification. By giving forward secure ID-based ring signature method security level of ring signature is highly increased. In this encryption method, if the secret key of any user has been compromised, previous generated signatures of all is included and the user still remains valid. If a secret key of single user has been compromised it is impossible to ask all data owners to re-authenticate their data. It is particularly important to any large scale data sharing system and it is very effective and does not require any pairing operations. The user secret key is one, while the key update process requires an exponentiation. This scheme is useful specially to those require authentication and user privacy.

D. Proxy Re-encryption:

Proxy Re-encryption is one more technique that supports secure data sharing and confidential data sharing in the Cloud. Proxy Re-encryption allows a semi-trusted proxy with a re-encryption key to convert a cipher-text under the data owner's public key into another cipher-text that can be decrypted by other user's secret key.

A user, Alice, encrypts her data using her public key. Alice sends the encrypted data to a proxy, when she wants to share her data with another user, say Bob. The proxy then converts the data encrypted under Alice's public key into data that is encrypted under Bob's public

key and sends this to Bob. Bob is able to use his private key to decrypt the cipher-text and reveal the data.

E. Cipher Text-Policy Attribute Based Encryption(CP-ABE):

Sphurti Atram,et al [4] introduced the concept of modified form of Attribute Based Encryption called Cipher text Policy Attribute Based Encryption. In this method, attribute policies are connected with data, which are associated with the keys and only those keys that the associated attributes satisfy the policy associated with the data which are able to decrypt the data. CP-ABE works in the inverse way of KP-ABE. In this method, the cipher text is associated with an access tree structure and each user secret key is embedded with a set of attributes. Key Policy and Cipher text policy based Encryption are the two different methods of attribute based encryption. The authority user can run the algorithm Setup and Key Generation to generate system SK, PK, and user secret keys. Only authorized users are able to decrypt by calling the algorithm Decryption. Here, each user is associated with a set of attributes. The users secret key is generated based on their attributes. While encrypting a message, the encrypter specifies the threshold access structure for their attracted attributes. This message is then encrypted based on this access structure such that only those whose attributes satisfy the access structure can decrypt it. With CP-ABE technique, encrypted data can be kept confidential and secure against collision attacks [4].
Cipher text policy based Attribute Based Encryption scheme consists of following four algorithms:

1. Setup: This algorithm takes as input a security parameter k and returns the public key PK as well as a system master secret key MSK. PK is used by message senders for encryption. SK is used to generate user secret keys and is known only to the authority.

2. Encrypt: This algorithm gets as input the public parameter PK, a message M, and an access structure T. It gives output as the cipher text CT.

3. Key-Gen: This algorithm takes as input a set of attributes associated with the user and the master secret key MSK. It outputs a secret key SK that enables the user to decrypt a message encrypted under an access tree structure T if and only if matches T.

4. Decrypt: This algorithm takes as input the cipher text CT and a secret key SK for an attributes set. It gives the message M if and only if satisfies the access structure associated with the cipher text CT. In CP-ABE depends how attributes and policy are associated with cipher texts and users‟ decryption keys. In a CP-ABE scheme, a cipher text is associated with a monotonic tree access structure and a user's decryption key is associated with set of attributes. In this scheme, the roles of cipher text and decryption keys are switched as that in KP-ABE.

F. Multi-Party Searchable Encryption(MPSE):

Qiang Tang et.al [8] suggested a searchable encryption namely multi-party searchable encryption (MPSE). It enables users to selectively permit each other to search in their encrypted data. He proposed a new scheme with provable security. A security model for MPSE provides stronger security guarantee than that from [9]. In the construction of MPSE, authorization is permitted on index level, for each of her indexes. Example Alice can make a decision whether Bob can search or not that is if all keywords try by authorized Bob then Alice supports authorize Bob to look for a subset of keywords in her indexes and also colluded with Bob can recover the keyword in all Alice's search queries. In this method, Alice can find out a problem of single trapdoor search for all indexes that have been authorized by her.

IV. CONCLUSIONS

In this paper we have overviewed different encryption schemes that can be used in cloud computing systems are flexible, scalable and fine grained access control. The main issue with data sharing in the cloud is the privacy and security. Various encryption techniques are discussed in this paper to support privacy and secure data sharing such as Data sharing and accessing through cloud. In ABE scheme, there are both the 'secret key' and 'cipher text' are associated with a set of attributes. ABE is again changed into KP-ABE that provides fine grained access control. In Key policy attribute based encryption, attribute policies are associated with keys and also the data is associated with the attributes. The Keys are associated with the policy that is satisfied by the attributes can decrypt the data. The CP-ABE scheme differs from KP-ABE in such a way that in CP-ABE, cipher text is associated with an access tree structure and each user secret key is embedded with a set of attributes. Attribute policies are associated with data and attributes which are again associated with keys and only those keys that the associated attributes satisfy the policy associated with the data are able to decrypt the users data.

REFERENCES

[1] Junzuo Lai,Deng, R.H, Chaowen Guan, Jian Weng, "*Attribute-Based Encryption With Verifiable Outsourced Decryption* ",Information Forensics and Security, IEEE Transactions on , vol.8, no.8,Aug. 2013, pp.1343,1354.

[2] Mohit Marwaha1, Rajeev Bedi, "*Applying Encryption Algorithm for Data Security and Privacy in Cloud Computing*", International Journal of Computer Science Issues, Vol. 10, Issue 1, No 1, January 2013.

[3] Saravana Kumar Na, Rajya Lakshmi G.Vb, Balamurugan Ba," *Enhanced Attribute Based Encryption for Cloud Computing,"* International Conference on Information and Communication Technologies, Procedia Computer Science Vol.46, 2015,
689 – 696.

[4] Sphurti Atram, N. R. Borkar," *A Review Paper on Attribute-Based Encryption Scheme in Cloud Computing*," International Journal of Computer Science and Mobile Computing, Vol. 6, Issue. 5, May 2017,260 – 266.

[5] V. Goyal, O. Pandey, A. Sahai, and B. Waters, *"Attribute-Based Encryption for Fine-grained Access Control of Encrypted Data*," In Proc. of CCS'06, Alexandria, Virginia, USA, 2006.

[6] R.Ostrovsky, A. Sahai, and B. Waters, *"Attribute-based encryption with non-monotonic access structures*," In Proc. of CCS'06, New York, NY, 2007.

[7] Xinyi Huang, Joseph K. Liu, Shaohua Tang, IEEE, Yang Xiang, Kaitai Liang, Li Xu, and Jianying Zhou, "*Cost-Effective Authentic and Anonymous Data Sharing with Forward Security*," IEEE Transactions On Computers, Vol. 64, No. 4, April 2015.

[8] Xuefeng Liu, Yuqing Zhang, Boyang Wang, and Jingbo Yan, "Mona: *Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud*," IEEE Transactions On Parallel and Distributed Systems, Vol. 24, No. 6, June 2013.

[9] Kaiping Xue and Peilin Hong, "*A Dynamic Secure Group Sharing Framework in Public Cloud Computing,*" Citation information: DOI 10.1109/TCC.2014.2366152, IEEE Transactions on Cloud Computing.

