International Conference on Innovative Applications in Engineering and Information Technology (ICIAEIT-2017)

International Journal of Advanced Scientific Technologies ,Engineering and Management Sciences (IJASTEMS-ISSN: 2454-356X) Volume.3,Special Issue.1,March.2017

Secure Data Sharing, Collaboration and User Revocation In Cloud Computing

A.Jyothi
Anurag Group of Institutions
Ghatkesar, Hyderabad, India

Dr. B. Indira
Kasturba GandhiDegree& PG
College for Women, Secundrabad, India

Abstract-Cloud computing provides many services and also convenient ways of data sharing and collaboration. Data in the cloud can be accessed by an individual or shared among the group and since the data often contains valuable information, security of the data plays a crucial role. Several security mechanisms have been proposed for secure data sharing .This paper reviews some security mechanisms along with attribute based encryption (ABE) where the data is encrypted even prior to its storage on the cloud and also the issue of revoked users, where the revoked user should be restrained to access the data stored on the cloud

Index Terms- Data sharing, Revoked users, Encryption, Security

I.INTRODUCTION

Cloud computing is an emerging paradigm which provides the access to the shared pool of resources. The resources might be computing capacity, network services, storage etc. Due to the advantage of economy of cloud, many organizations are utilizing the services provided by the major cloud service providers like Amazon, Azure, Rackspace etc. The emerging trend in utilizing the services of cloud is sharing of data. The data especially sensitive data which is outsourced to the cloud, poses many challenges such as data security and data access control. Data which is to be outsourced is encrypted and stored on the cloud; any user who wants to access the data should decrypt the data. This paper presents various recent approaches in sharing of data as well as revocation techniques.

II. DATA SHARING AND COLLABORATION

A.ATTRIBUTE BASED ENCRYPTION

In 1984 Shamir proposed a novel cryptographic scheme, Identity Based Encryption (IBE) (1). The main motive was to simplify certificate management system, which enables any pair of users to communicate securely and to verify each other's signatures without exchanging private or public keys, without keeping key directories, and without using the services of a third party. The security of IBE was left as an open problem

An extension to Identity Based Encryption is given by Clifford Cocks (2), this scheme is based on Quadraticresidues. If Bob wants to send an encrypt message to Alice, he first generates a transport key and uses it to encrypt the data using symmetric encryption. He sends to Alice each bit of the transport key. This scheme will be expensive if the transport key is long and is also vulnerable to an adaptive cipher text attack because the transport key is established one bit at a time

D. Boneh and M. Franklin. Proposed another IBE based on Weil pairing (3), this scheme has chosen ciphertext security

Sahai and waters (4) proposed Fuzzy Identity Based Encryption which is derived from Identity Based Encryption Fuzzy- IBE has two important applications .The first is IBE that uses biometric identities. User’s identity is described by several attributes and then encryption is done using their biometric identity. Since biometric measurements are noisy, existing IBE systems will not work. However, the error-tolerance property of Fuzzy-IBE allows for a private key to decrypt a ciphertext encrypted with a slightly different measurement of the same biometric.

Secondly, Fuzzy IBE can be used for an application “Attribute Based Encryption” is an application of identity based encryption, is an access control mechanism where a user or a piece of data has attributes associated with it. An access control policy is defined and if the attributes satisfy the access control policy then the user will get the access to the data. The access control policy is defined as an access tree where the leaf nodes represent attributes and the interior nodes represent the threshold gates

According to Goyal V, Pandey O, Sahai A, Waters (5), One drawback of encrypting data is that data can be selectively shared at a coarse-grained level, for fine-grained sharing of encrypted data, Key-Policy Attribute-Based Encryption(KP-IBE)is used

There are two kinds of ABE

Key-Policy ABE(KP-ABE)-With the private key of the user the access control policy is stored, when any user want to get the data can decrypt the data only if the user satisfies the attributes in the access control policy

Ciphertext-Policy ABE (CP-ABE)-It is the converse of KP-ABE.The access control policy is stored with the data and the attributes are stored in the user's key

CP-ABE is used by Tu S, Niu S, Li H, and Xiao-ming (6) in the context of enterprise applications; it allows fine grain access control and revocation. This scheme is secure against chosen plaintext attacks but places heavy computation overhead.

B.PROXY RE-ENCRYPTION

Proxy Re-encryption is another technique for secure sharing of data. PRE is initially introduced by y Blaze, Bleumer and Strauss(7)It allows a proxy with re-encryption key to translate the cipher text under the data owner's public key into another cipher text ,which can be decrypted with private keys of the user.

In this scheme at any of the stage, the proxy will be unable access the plain text but,this scheme suffers from collusion attack such that the proxy can reveal the data owner's private key by colluding with the user, it is bidirectional and useful when the trust relationship between the users is mutual.

Dodis-Ivan (8) has differentiated proxy functions as bi-directional and unidirectional and also proposed an unidirectional proxy encryption scheme.

One exception is the Dodis-Ivan IBE scheme, where the global secret that decrypts *all* cipher texts is shared between the proxy and the user. Thus, the user needs to store only a single secret, but an obvious drawback is that when the proxy and any user in the system collude, they can decrypt everyone else's message also.

In view of costly certificate management overhead in traditional public key encryption, Green et al.(8) introduced the notion of identity based proxy re-encryption (IB-PRE) scheme by incorporating the idea of PRE and ID-based encryption They gave the first concrete construction of the first ID-PRE scheme based on the bilinear pairing. Their PRE scheme is unidirectional, multi-use and non-interactive but not collusion-resistant

Tran et al. (14) uses the idea of Proxy Re-encryption scheme where the dataowner's private key is divided into two parts. One half is stored in the data owner'smachine while the other is stored in the Cloud proxy. The data owner encrypts thedata with half of his private key, which then gets encrypted again by the proxy usinghis other half of the key. When the data owner wishes to revoke a user from accessing the data, he simply informs the Cloud proxy to remove the user's key piece.

The main strength with this scheme is that it doesn't require re-encryption if a user's rights are revoked and hence saves the computation costs, only users with granted access rights can view the original plaintext.

However, the main problem with this scheme is that of collusion attacks; if a revoked user and the proxy collude, that user then has access to the other entire users private keys in the group. Also, the proxy may suffer from too many encryption and decryption operations.

C.HYBRID ABE AND PRE

ABE and Proxy Re-encryption have also been used in combination with each other to provide extra security and privacy for data sharing and collaboration in the Cloud.
.

Yu et al. (13) was one of the first works, which combined ABE, Proxy Re-Encryption and lazy encryption schemes for Cloud privacy and security. The schemeworks by data owner encrypting his data using a symmetric key and then encryptingthe symmetric key using a set of attributes according to KP-ABE scheme. The data owner assigns an access structure and its corresponding secret key and distributes this to the new user, when he joins the system. To revoke a user, the data owner determines the minimum number of attributes, which will never satisfy the revoked user's access structure and update these as necessary. All the remaining users' secret keys will also be updated. Due to heavy computational overhead, proxy re-encryption is introduced to allow the Cloud to carry out these tasks

Yang and Zhang (12) also proposed a combination of the ABE scheme and Proxy Re-encryption scheme to enable secure data sharing in the Cloud. This technique ensures that data is kept confidential against the Cloud and from any unauthorized users. When a user is revoked access rights, the data owner simply informs the Cloud to remove that user's entry in the authorization list and hence is computationally efficient.

However, this scheme does not deal with the scenario where a revoked user rejoins the group with different access privileges. The revoked user still has the decryption keys corresponding to ABE and hence in theory can regain access to data he is not allowed to.
InCombination of Clock based proxy re-encryption(C-PRE) and CP-ABE scheme(11),a key is shared between the data owner and the cloud and this key is used to calculate the PRE keys based on the internal clock of the cloud .The

cloud acts as a proxy and re-encrypts the cipher texts using the PRE Keys. Each user in the group is associated with set of attributes and eligible time, which determines how long a user can access the data. Only the users whose attributes satisfy the control structure and the eligible time can decrypt the data.

With the above approaches the data owner can outsource the data on to cloud and be assured that sharing of the data is more secure and confidential.

When the data is shared by a group of users, only authorized users should able to access the data. If any user in the group is revoked due to any of the reasons such as an employee fired from organization, malicious user etc., due to the security concerns should not be allowed to access or decrypt the data.

Various techniques have been proposed for revocation of the users. Some of them are

III. USER REVOCATION

A.REVOCATION USING ABE

In this scheme revocation is done using CP-ABE (6).The users in a group are assigned a set of attributes in their secret key and are distributed to the user, when a user is revoked,then the data is re-encrypted making the secret key of the revoked user useless, this scheme is secure but involves more computational overhead as, the data needs to be encrypted whenever there is an user revocation.

B.REVOCATION USING PRE

Revocation is done using the idea of proxy re-encryption(13) ,data owner's private key is divided into two parts .one half part is stored at data owner's place and other half is stored in the cloud proxy, the owner encrypts the data with the key available with him and the cloud encrypts the data again using the other part of the key .Any user who has access rights can decrypt the data with two parts of the key .When the data owner wishes to revoke any user, informs cloud to remove the user's key piece from the cloud, this method of revocation does not require re-encryption of data thereby reducing the computational cost but, likely hood of collusion attacks are more and also the cloud proxy may suffer from too many encryption and decryption operations.

C.REVOCATION USING C-PRE AND COMBINED CP-ABE

This scheme(11) is a combination of Clock based proxy re-encryption and attribute based encryption. Each user is associated with set of attributes and eligible time, attributes and the time does not satisfy when the user is revoked.The advantage of this technique is re-encryption which is delegated to the cloud instead of data owner. When very large data files are considered this scheme is not very efficient.

CONCLUSION

Data sharing and collaboration has become prominent in the current day scenario, therefore much importance is given to the security of data stored in the cloud. Since the data is dynamic, many security and access control schemes are proposed, in this paper, few recent approaches in data security and also some access control mechanisms for revoked usershave been presented.

REFERENCES

[1] A. Shamir, "Identity-based cryptosystems and signature schemes", in Advances in Cryptology – Crypto '84, Lecture Notes in Computer Science, Vol. 196, Springer-Verlag, pp. 47–53, 1984

[2] 2. Clifford Cocks. An identity based encryption scheme based on quadratic residues. In *IMA Int. Conf.*, pages 360–363, 2001.

[3] 3. D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," SIAM Journal on Computing, vol. 32, no. 3, pp. 586– 615, 2003

[4] 4.A. Sahai and B. Waters. Fuzzy Identity Based Encryption. In *Advances in Cryptology – Eurocrypt*, volume 3494 of *LNCS*, pages 457–473. Springer, 2005.

[5] 5. Goyal V, Pandey O, Sahai A, Waters B (2006) Attribute-based encryption for fine-grained access control of encrypted data. 13th ACM conference on computer and communications security (CCS '06) 2006, pp 89–98.3.

[6] 6.Tu S, Niu S, Li H, Xiao-ming Y, Li M (2012): Fine-grained access control and revocation for sharing data on clouds. IEEE 26th international parallel and distributed processing symposium workshops and PhD forum (IPDPSW) 2012, pp 2146–2155.

[7] 7..M. Blaze, G. Bleumer, and M. Strauss, "Divertible pro-tocols and atomic proxy cryptography," in Advances in Cryptology–EUROCRYPT'98. Springer, 1998, pp. 127–144.

[8] 8YevgeniyDodis and Anca Ivan. Proxy cryptography revisited. In Proceedings ofthe Tenth Network and Distributed System Security Symposium, February 2003.

[9] 9 .M. Green and G. Ateniese, "Identity-based proxy reencryption," in Proceedings of the 5th International Conference on Applied Cryptography and Network Security. Springer, 2007, pp. 288–306.

[10] 10. Wang X, Zhong W (2010) A new identity based proxy re-encryption scheme. International conference biomedical engineering and computer science (ICBECS) 2010:145–153

[11] 11. Liu Q, Wang G, Wu J (2012) Check-based proxy re-encryption scheme in unreliable clouds. 41st international conference on parallel processing workshops (ICPPW) 2012, pp 304–305.

[12] 12.Yang Y, Zhang Y (2011) A generic scheme for secure data sharing in cloud. 40th international conference parallel processing workshops (ICPPW) 2011, pp 145–153.

[13] 13.Yu S, Wang C, Ren K, Lou W (2010) Achieving secure, scalable, and fine-grained data access control in cloud computing. In: INFOCOM, 2010 proceedings IEEE, pp 1–9

[14] 14.Tran DH, Nguyen HL, Zha W, Ng WK (2011) Towards security in sharing data on cloudbased social networks. 8th International conference on information, communications and signal processing (ICICS) 2011, pp 1–5.