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.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department Of CSE, JayaShriram Group Of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Privacy-Preserving Data Sharing for Dynamic Groups in the Cloud: A Survey

S.Mythili[1], M.Velmurugan[2]

M.E, Department of CSE, Vivekandha Institute of Engineering and Technology for Women, Trichengode, India[1]

Asst Prof, Department of CSE, Vivekandha Institute of Engineering and Technology for Women, Trichengode*,* India[2]

Abstract--In recent years, the use of cloud computing in real life applications has increased rapidly. It provides an efficient solution for sharing group resource among cloud users. Sharing data in a multi-owner manner while preserving data and identity privacy from an un-trusted cloud is still a challenging issue, due to the frequent change of the membership. This paper surveys new granted users can directly decrypt data files uploaded before their participation without contacting with data owners. This scheme is able to support dynamic groups efficiently. User revocation can be achieved through a novel revocation list without updating the secret keys of the remaining users. Finally these papers summarize and conclude with the different algorithms and technique

Index Terms–Cloud computing, Data sharing, Privacy preserving, dynamic groups

I. INTRODUCTION

Cloud computing [1] is a technology that uses the internet and central remote servers to maintain data and applications. Cloud computing allows consumers and businesses to use applications without installation and access their personal files at any computer with internet access. This technology allows for much more efficient computing by centralizing storage, memory, processing and bandwidth. Cloud computing is a comprehensive solution that delivers IT as a service.

One of the most fundamental services offered by cloud providers is data storage. Consider a practical data application, a company allows its staffs in the same group or department to store and share files in the cloud. By utilizing the cloud, the staffs can be completely released from the troublesome local data storage and maintenance. To preserve data privacy, a basic solution is to encrypt data files, and then upload the encrypted data into the cloud [2]. Designing an efficient and secure data sharing scheme for groups in the cloud is not an easy task due to the following challenging issues.

First, identity privacy is one of the most significant obstacles for the wide deployment of cloud computing Without the guarantee of identity privacy, users may be unwilling to join in cloud computing systems because their real identities could be easily disclosed to cloud providers and attackers.

Second, it is highly recommended that any member in a group should be able to fully enjoy the data storing and sharing services provided by the cloud, which is defined as the multiple-owner manner. Compared with the single-owner manner [3], where only the group manager can store and modify data in the cloud, the multiple-owner manner is more flexible in practical applications.

The major challenges which are to be considered in cloud computing are

- Cost
- Constant Internet connection

- Stored data might not be secure

II. LITERATURE REVIEW

A. PLUTUS

The first developed Cryptographic storage system is the PLUTUS [2] that enables secure file sharing without placing much trust on the file servers .It makes novel use of cryptographic primitives to protect and share files. PLUTUS features highly scalable key management while allowing individual users to retain direct control over who gets access to their files. Plutus provide basic file system security features are to detect and prevent unauthorized data modifications, to differentiate between read and write access to files, and to change users' access privileges.

Plutus groups files into file groups so that keys can be shared among files in a file group without compromising security. File groups serve as a file aggregation mechanism to prevent the number of cryptographic keys a user manages from growing proportional to the number of files. The mechanisms of PLUTUS is to reduce the number of cryptographic keys exchanged between users by using file groups, distinguish file read and write access, handle user revocation efficiently, and allow an un-trusted server to authorize file writes. The major drawback of this technique is that the keys, needs to be updated and distributed for a user revocation had the problem in PLUTUS.

B. SiRiUS

To overcome these drawbacks, Securing remote un-trusted storage (SiRiUS) [3] was developed by extending the PLUTUS. SiRiUS assumes the network storage is un-trusted and provides its own read-write cryptographic access control for file level sharing. Key management and revocation is simple with minimal out-of-band communication. File system are supported by SiRiUS using hash tree constructions. SiRiUS contains a novel method of performing file random access in a cryptographic file system without the use of a block server. Zero-Interaction Authentication (ZIA) aims to secure mobile devices even against physical attacks. ZIA implements file access control via a cryptographic file system that communicates with a physical authentication token.

Public key cryptography is used to authenticate a physical token to the mobile device. File sharing is implemented using symmetric ciphers. SiRiUS can use ZIA to secure the master keys on the client machine. The use of SiRiUS is compelling in situations where users have no control over the file server (such as Yahoo!). SiRiUS is the most that can be done to secure an existing network file system without changing the file server or file system protocol. Key management in SiRiUS is very simple because each file keeps track of its own file keys for access control. All users only need to keep track of two keys; the MSK and the MEK. There is no out of-band communication if Identity Based encryption and signature schemes are used. Otherwise, a small amount of out-of-band communication is required in order to obtain public keys. Extensions to SiRiUS include large scale group sharing using the NNL key revocation construction. This Sirius does not support for Deleting File System Contents, Seizing File System Control and d-files Rollback.

C. PROXY RE-ENCRYPTION

The next developed Scheme is proxy re-encryption [4], in which a semi trusted proxy converts a cipher text without seeing the underlying plaintext. It predicted that fast and secure re-encryption for managing encrypted file systems. Although efficiently computable, the wide-spread adoption of BBS re-encryption has been hindered by considerable security risks.

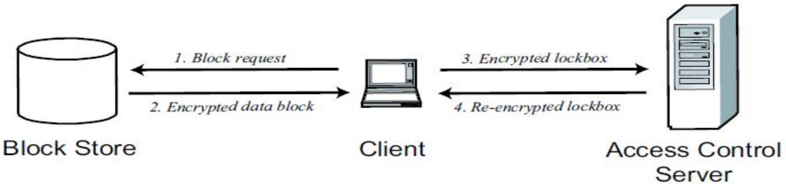

Figure 1: Encrypted file storage

Efficient proxy re-encryption schemes provide security improvements over earlier approaches. Operation of the proxy re-encryption files system. The user's client machine fetches encrypted blocks from the block store. Each block includes a lockbox encrypted under a master public key. The client then transmits lockboxes to the access control server for re-encryption under the user's public key. If the access control server possesses the necessary re-encryption key, it re-encrypts the lockbox and returns the new cipher text. The client can then decrypt the re-encrypted block with the user's secret key. It described a file system which uses an un-trusted access control server to manage access to encrypted files stored on distributed, un-trusted block stores. It used proxy re-encryption to allow for access control without granting full decryption rights to the access control server. The implementation represented the first experimental implementation and evaluation of a system using proxy re-encryption.

The primary advantage of this schemes is that they are unidirectional (i.e., Alice can delegate to Bob without Bob having to delegate to her) and do not require delegators to reveal all of their secret key to anyone—or even interact with the delegate—in order to allow a proxy to re-encrypt their cipher texts. This scheme, only a limited amount of trust is placed in the proxy. For example, it is not able to decrypt the ciphertexts it re-encrypts and it proveschemes secure even when the proxy publishes all the re-encryption information it knows. This enables a number of applications that would not be practical if the proxy needed to be fully trusted.

D. ATTRIBUTE-BASED ENCRYPTION

To overcome the drawbacks in PROXY RE-ENCRYPTION, Attribute based encryption (ABE) [6] was developed.KP-ABE, data are associated with attributes for each of which a public key component is defined. The encrypt or associates the set of attributes to the message by encrypting it with the corresponding public key components. Each user is assigned an access structure which is usually defined as an access tree over data attributes, User secret key is defined to reflect the access structure so that the user is able to decrypt a cipher text if and only if the data attributes satisfy the access structure.

E. CP-ABE

In order to overcome the drawbacks in PROXY RE-ENCRYPTION, Cipher text-Policy Attribute-Based Encryption (CP-ABE) [5] was developed by extending the existing CP-ABE. As PROXY RE-ENCRYPTION, the CP-ABE one cloud creates a cipher text that can be opened only if the attributes of a user match a policy. CP-ABE systems that allow for complex policies would have a number of applications. An important example is a kind of sophisticated Broadcast Encryption, where users are described by (and therefore associated with) various attributes. Cipher texts are associated with sets of attributes, whereas user secret keys are associated with policies. This setting has a number of natural applications. Another possibility is to have the reverse situation: user keys are associated with sets of attributes, whereas cipher texts are associated with policies. This is called as Cipher text-Policy Attribute-Based Encryption (CP-ABE) systems. CP-ABE systems that allow for complex policies would have a number of applications. An important example is a kind of sophisticated Broadcast Encryption, where users are described by various attributes. Then, one could create a cipher text that can be opened only if the attributes of a user match a policy. For instance, in a military setting, one could broadcast a message that is meant to be read only by users who have a rank of Lieutenant or higher.

It presented three constructions within this framework. The first system is proven selectively secure under an assumption that called the decisional Parallel Bilinear Diffie-Hellman Exponent (PBDHE) assumption which can be viewed as a generalization of the BDHE assumption. Next two constructions provide performance tradeoffs to achieve provable security respectively under the (weaker) decisional Bilinear-Diffie-Hellman Exponent and decisional Bilinear Diffie-Hellman assumptions. The Contribution presents a new methodology for realizing Ciphertext-Policy ABE systems from a general set of access structures in the standard model under concrete and non-interactive assumptions. Both the ciphertext overhead and encryption time scale with O (n) where n is the size of the formula. In addition, decryption time scales with the number of nodes. CP-ABE technique which allows any member in a group to share data with others. CP-ABE is not support for dynamic groups.

F. KP-ABE

To overcome the drawbacks in CP-ABE Key Policy Attribute-Based Encryption (KP-ABE) [7] was developed. KP-ABE is a public key cryptography primitive for one-to-many communications. In KP-ABE, data are associated with attributes for each of which a public key component is defined. The encrypt or associates the set of attributes to the message by encrypting it with the corresponding public key components. Each user is assigned an access structure which is usually defined as an access tree over data attributes, User secret key is defined to reflect the access structure so that the user is able to decrypt a cipher text if and only if the data attributes satisfy the access structure.KP-ABE Support to Fine-grained access control systems facilitate granting differential access rights to a set of users and allow flexibility in specifying the access rights of individual users.

Several techniques are used for implementing fine grained access control. Access control relies on software checks to ensure that a user can access a piece of data only if the authorized user can to do. This situation is not particularly appealing from a security standpoint. For example, as a result of a software vulnerability exploit, the potential for information theft is immense. Furthermore, there is always a danger of “insider attacks” wherein a person having access to the server steals and leaks the information .In these techniques, the data is stored on the server in an encrypted form while different users are still allowed to decrypt different pieces of data per the security policy. This effectively eliminates the need to rely on the storage server for preventing unauthorized data access. The issue of user revocation was notaddressed in KP-ABE.

G. DYNAMIC BROADCAST ENCRYPTION

To overcome the drawbacks in CP-ABE, aDynamic broadcast encryption [6] [8] was developed. It mainly focuses on any member of the group can sign messages, but the resulting signature keeps the identity of the signer secret. In some systems there is a third party that can trace the signature, or undo its anonymity, using a special trapdoor. Some systems support revocation where group membership can be selectively disabled without affecting the signing ability of unrevoked members.

Broadcast system is dynamic when

- The system setup as well as the cipher text size are fully independent from the expected number of users or an upper bound
- A new user can join anytime without implying a modification of preexisting user decryption keys,
- The encryption key is unchanged in the private-key setting or incrementally updated in the public-key setting, meaning that this operation must be of complexity at mostO (1).

Main contributions of dynamic broadcast encryption are the broadcast cipher text or the decryption key containing all the information required by the Receiver to decrypt is of constant size and the group manager can dynamically include new members while preserving computed information: In particular, user decryption keys need not be recomputed, the morphology and size of cipher texts are unchanged and the group encryption key requires minimal or no modification. A dynamic broadcast encryption scheme involves two authorities: a group manager and a broadcaster. The group manager grants new members access to the group by providing to each new member a public label and a decryption key. The generation of public label and decryption is performed using a secret manager key. The broadcaster encrypts messages and transmits these to the whole group of users through the broadcast channel. The efficient clustering with proper cluster head selection based on the distance between different nodes. It aims at number of revocation mechanisms for group signatures have been the drawback here is that revocation for a group is not addressed efficiently.

H. GROUP SIGNATURE

By resolving the problems in CP-ABE, GROUP SIGNATURE [10] was developed. Group signatures provide anonymity for signers. Any member of the group can sign messages, but the resulting signature keeps the identity of the signer secret. Short group signatures whose length is under 200 bytes that offer approximately the same level of security as a regular RSA signature of the same length. The security of the scheme is based on the Strong Diffie-Hellman (SDH) assumption in groups with a bilinear map, which introduced a new assumption called the linear assumption.

Group signature must satisfy following three properties

- Correctness, which ensures that honestly-generated signatures verify and trace correctly;
- Full-anonymity, which ensures that signatures do not reveal their signer's identity; and
- Full-traceability, which ensures that all signatures, even those created by the collusion of multiple users and the group manager, trace to a member of the forging coalition.

This system is based on a new Zero-Knowledge Proof of Knowledge (ZKPK) of the solution to an SDH problem. It converts this ZKPK to a group signature via the Fiat-Shamir heuristic and proves security in the random oracle model. The security proofs use a variant of the security model for group signatures proposed by Bellare, Micciancio, and Warinschi. A number of revocation mechanisms for group signatures are developed. The number of revoke users without affecting the signing capability of other users. The Revocation Authority publishes a Revocation List containing the private keys of all revoked users. Brickell proposed an alternate mechanism where revocation messages are only sent to signature verifiers, so that there is no need for unrevoked signers to update their keys. Similar mechanisms were also considered by Ateniese and Kiayias this refer to this as Verifier-Local Revocation (VLR) group signatures. Boneh and Shacham show how to modify our group signature scheme to support this VLR revocation mechanism.

III. CONCLUSION

In this paper, we have surveyed different security scheme in Cloud Computing in terms of its performance and data sharing scheme. The major aim of data sharing scheme is to share data for dynamic groups in an un-trusted cloud. A user is able to share data with others in the group without revealing identity privacy to the cloud. More specially, efficient user revocation can be achieved through a public revocation list without updating the private keys of the remaining users and new users can directly decrypt files stored in the cloud before their participation. Moreover, the storage overhead and the encryption computation cost are constant. It supports efficient user revocation and new user joining in the group.

IV. REFERENCES

1. M. Armbrust, R. Fox, Griffith, A.D.Joseph, R.H. Katz, 'A View of Cloud Computing' -Comm. ACM, vol. 53, no. 4, pp. 50-58.

2. M. Kallahalla, E. Riedel, and K. Fu,(2003) 'Plutus: Scalable Secure File Sharing on Un-trusted Storage,'- Proc.USENIX Conf. File And Storage Technologies, pp. 29-42.

3. E. Goh, H. Shacham, N. Modadugu, and D.Boneh, (2003) 'Sirius: Securing Remote Un-trusted Storage,'- Proc. Network and DistributedSystems Security Symp. (NDSS), pp. 131-145.

4. G. Ateniese, and S. Hohenberger, (2005) 'Improved Proxy Re-Encryption Schemes with Applications to SecureDistributed Storage,'- Proc. Network and Distributed Systems Security Symp. (NDSS), pp. 29-43.

5. B.Waters,(2008) "Cipher text-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization,"- Proc.Int'l conf practice and theory in public key cryptography conf public key cryptography, http://eprint.iacr.org/2008/290.pdf.

6. V. Goyal, O. Pandey, A. Sahai, and B. Waters, (2006) 'Attribute-Based Encryption for Fine-Grained Access Control of EncryptedData,'- Proc.ACM Conf. Computer and Comm. Security (CCS), pp.89-9.

7. D. Boneh and M. Franklin, (2001)'Identity-Based Encryption from the Weil Pairing,'- Proc. Int'l Cryptology Conf. Advancesin Cryptology (CRYPTO), pp. 213-22.

8. D. Boneh, X. Boyen, and H. Shacham, (2004) 'short Group Signature,' -Proc. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO), pp. 41-55.

9. D. Chaum and E. van Heyst, (1991) 'Group Signatures,'- Proc. Int'lConf.Theory and Applications of Cryptographic Techniques (EUROCRYPT), pp. 257-265.