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, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Robust Data Authenticity and Group Signature Mechanism for Enhanced Cloud Security Process

D.Sharmili[1], B. Palani Chelvam[2]

PG Student, Department of CSE, Syed Ammal Engineering College, Ramanathapuram, TamilNadu, India[1]

Assistant Professor, Department of CSE, Syed Ammal Engineering College, Ramanathapuram, TamilNadu, India[2]

ABSTRACT— Cloud storage enables users to remotely store their data and enjoy the on-demand high quality cloud applications without the burden of local hardware and software management. In order to achieve a secure and dependable cloud storage service, a secure multi-owner data sharing scheme is proposed according to which any user in the group can securely share data with others by the un-trusted cloud. For reducing the execution time of the keys generation at the user or data owner side, the Group manager is used, who is responsible for generating the group keys for communication between the data owners in the cloud. In addition to the validation of data authenticity by secure group signature mechanism, it is also used for signature generation and verification procedure for enhanced data integrity mechanism to the data being shared in the cloud storage. Thus provides secure and privacy-preserving access control to users, which guarantees any member in a group to anonymously utilize the cloud resource. Moreover, Initiator is introduced which acts as the middleware between the group manager and the data owners for sending the key generation request to Group manager with a list of group members, and provides key confidentiality for enhanced security of cloud data.

KEYWORDS— Cloud computing, data sharing, privacy-preserving, access control, dynamic groups

I. INTRODUCTION

Numerous trends are opening up the era of Cloud Computing, which is an Internet-based development and use of computer technology. The increasing network bandwidth and reliability yet flexible network connections make it even possible that users can now subscribe high quality services from data and software that reside solely on remote data centers. Moving data into the cloud offers great convenience to users since they don't have to care about the complexities of direct hardware management. In cloud computing, the cloud service providers (CSPs) are responsible for delivering various services to cloud users. Users can enjoy high-quality services by migrating the local data management systems into the corresponding cloud servers. However, such cloud servers managed by cloud providers are not fully trusted by users especially when the data files stored in the cloud are sensitive and confidential. Thus to preserve data privacy, a primitive solution is to first encrypt data files, and then to upload the encrypted data into the cloud [2]. But designing an efficient and secure data sharing scheme for groups in the cloud is somewhat a complex task due to the following issues.

1) Identity privacy is one of the most important obstacles for the deployment of cloud computing. If no guarantee is provided for identity privacy, then users may hesitate to join in cloud computing environment as their real identities could be easily disclosed to cloud providers and attackers. At the same time, unconditional identity privacy may lead to the violation of privacy. Therefore in such cases, traceability, which enables the group manager to reveal the original identity of a user, is highly essential.

2) Any member in a group should be able to fully utilize the data storing and sharing services provided by the cloud, which is termed as multiple-owner manner. While in the single-owner manner [3], only the group manager is

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, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

allowed to store and modify data in the cloud. Thus, each user in the group can not only be able to read data, but also to modify his/her part of data in the entire data file shared by the group in the cloud.

3) Groups are normally dynamic in reality, e.g., new member participation and current member revocation in a single group. The change of membership makes secure data sharing in the cloud as extremely complex. That is on one hand, the system challenges newly granted users to learn the content of data files stored even before their participation, as it is impossible for new users to contact with corresponding data owners to obtain the respective decryption keys. And on the other hand, an efficient membership revocation mechanism is required without any update of the secret keys of the remaining users in order to minimize the complexity of key management.

To solve the challenges that are listed above, a secure multi-owner data sharing scheme for dynamic groups in the cloud is proposed. The main contributions of this paper are described as follows:

A secure multi-owner data sharing scheme is proposed in this paper. It implies that any user in the group can securely share data with others in the untrusted cloud and has the ability to support dynamic groups efficiently. Specifically, newly participated users can directly decrypt data files uploaded before their participation without contacting the corresponding data owners. The size and computation overhead of encryption are considered to be constant and are independent with the number of revoked users. Moreover, the real identities of data owners can be revealed by the group manager when disputes occur. Group manager distributes and efficiently allocates the public keys and authenticate by using digital signature process.

User revocation from a group is easily achieved by a revocation list without updating the secret keys of the remaining users. Thus the system provides secure and privacy-preserving access control to users and also guarantees that any member in a group can utilize the cloud resource.

The proposed system includes the introduction of INITIATOR. It acts as a middleware between the Group manager and the data owners for providing versatile authentication mechanism. The function of INITIATOR is to send a key generation request to Group manager with a list of group members. It results in providing Key Confidentiality to the shared data thereby enhances the data security. An advanced Authentication technique for group members is done by initiator rather than traditional authentication mechanisms such as username and password. Altogether a well secured key sharing with robust authentication process is achieved by the proposed system.

II. RELATED WORK

A new type of signature for a group of persons, called a group signature is described in [15], which states the following properties:

1) Only members of the group can sign messages.

2) The receiver can verify that it is a valid group signature, but cannot discover which group member made it.
3) If necessary, the signature can be "opened"(with or without the help of the group members), so that the person who signed the message is revealed.

A trusted authority (TA), chooses a public key system, gives each person a list of secret keys (these lists are all disjunctive) and publishes the complete list of corresponding public keys (in random order) in a Trusted Public Directory. Each person can sign a message with a secret key from his list, and the recipient can verify this signature with the corresponding public key from the public list. Each key will be used only once, otherwise signatures created with that key are linked. TA knows all the lists of secret keys, so that in case of dispute, he knows who made the disputed signature. If each person gets the same number of secret keys, then the length of the public key of this group signature scheme (i.e. the length of the Trusted Public Directory) is linear in the number of persons; but the number of messages a person can sign is fixed.

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, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Plutus, a cryptographic storage system is proposed in [4], which enables secure file sharing without placing much trust on the file servers. It 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 untrusted server to authorize file writes. By dividing files into file groups and encrypting each file group with a unique file-block key, the data owner can share the file groups with others through delivering the corresponding lockbox key, where the lockbox key is used to encrypt the file-block keys. The issues faced in this paper are heavy key distribution overhead for large-scale file sharing and File Block Key needs to be updated and distributed for a user revocation.

In [5], SiRiUS, a secure file system is designed to be layered over insecure network and P2P file systems. It assumes the network storage to be untrusted 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. Implementation of SiRiUS performs well relative to the underlying file system despite using cryptographic operations. In this system, files stored on the untrusted server include two parts: file metadata and file data. The file metadata implies the access control information including a series of encrypted key blocks, each of which is encrypted under the public key of authorized users. Thus, the size of the file metadata is proportional to the number of authorized users. However, Metadata needs to be updated for every user revocation and updation is complex for large scale sharing.

As more sensitive data is shared and stored by third-party sites on the Internet, there will be a need to encrypt data stored at these sites. One drawback of encrypting data is that it can be selectively shared only at a coarse-grained level (i.e., giving another party your private key). A new cryptosystem for fine-grained sharing of encrypted data that we call Key-Policy Attribute-Based Encryption (KP-ABE) is developed in [9]. In this cryptosystem, ciphertexts are labeled with sets of attributes and private keys are associated with access structures that control which ciphertexts a user is able to decrypt. This system simultaneously achieves fine-grainedness, scalability and data confidentiality for data access control in cloud computing. The goal is achieved by exploiting and uniquely combining techniques of attribute-based encryption (ABE), proxy re-encryption, and lazy re-encryption. However certain issues arises in this paper such as Data sharing is not done by multiple data owners and, Signature generation and verification process is not used.

Compared with the existing works, the proposed system offers unique features which are described as follows:

1) Any user within the group can store and share data files with others in the cloud.
2) The complexity of encryption and ciphertexts size, are independent with the number of revoked users in the group.
3) User revocation can be done without the need for updating the private keys of the remaining users.
4) New user can directly decrypt the required files stored in the cloud even before the participation.
5) Initiator reduces the overhead of Group manager by means of advanced authentication technique.

III. SYSTEM MODEL AND DESIGN GOALS

A. System Model

Fig. 1. System model

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, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

The system model consists of three entities: the cloud, a group manager and two or more group members as illustrated in Fig. 1. Although CSPs provide priced abundant storage services, the cloud is not fully trusted by users. In the existing system such as [3], [7], it is assumed that the cloud server is honest, that is the cloud server will not maliciously delete or modify user data due to the protection provided by the data auditing schemes proposed in [17], [18], but will somehow try to learn the content of the stored data and the identities of cloud users. Group manager takes charge of system parameters generation, user registration, user revocation, and revealing the real identity of a dispute data owner with the help of group key verification. Group members are a set of registered users that will store their private data into the cloud server and share them with others in the group where the group membership is supposed to be dynamically changing.

B. Initiator

Initiator acts as a middleware between the Group manager and the data owners for providing versatile authentication mechanism. The function of Initiator is to send a key generation request to Group manager with a list of group members thereby reduces the computation overhead in group key management. It also provides Key Confidentiality to the shared data and enhances the data security. An advanced Authentication technique for group members is done by initiator rather than traditional authentication mechanisms such as username and password. Altogether a well secured key sharing with robust authentication process is achieved by the proposed system.

C. Dynamic Broadcast Encryption

Broadcast encryption described in [16] involves a broadcaster to transmit encrypted data to a set of authorized users so that only a privileged subset of users can decrypt the data. Dynamic broadcast encryption allows the group manager to dynamically include new members and at the same time preserves the previously computed information. That is, user decryption keys need not be recomputed, the morphology and ciphertexts size are unchanged and at last the group encryption key need not requires any modification. This dynamic broadcast encryption is used as the basis for file sharing in dynamic groups.

D. Design Goals

This section describes the main design goals of the proposed scheme such as access control, data confidentiality, anonymity and traceability, and efficiency as follows:

1) Access control: Group members are able to access the cloud and make use of cloud resource for data operations. In addition, unauthorized users are restricted to access the cloud resource at any time, and revoked users cannot be able to use the cloud again once they are revoked.

2) Data confidentiality: To preserve data confidentiality, unauthorized users including the cloud must be incapable of learning the content of the stored data. An important issue for data confidentiality is to maintain its availability for groups that are dynamic in nature. That is, new users should decrypt the data stored in the cloud before their participation, and revoked users are unable to decrypt the data moved into the cloud after the revocation.

3) Anonymity and traceability: Anonymity guarantees that group members can access the data in the cloud without exposing their real identity. Although anonymity provides privacy for user identity, it also poses a potential inside attack risk to the system. Thus, to handle the inside attack, the Group manager must have the ability to reveal the real identities of data owners which is done by the proposed initiator.

4) Efficiency: Any group member can store and share data files with others in the group by the cloud. User revocation can be done without disturbing the activities of the remaining users. That is, the remaining users need not update their private key or re-encryption operations. Similarly newly participated users can learn all the content of the data files stored in the cloud even before their participation without contacting with the data owner. Altogether a well secured key sharing with robust authentication process is achieved by the proposed system.

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, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

IV. COMPONENTS

A. User Repository Creation

Each user or group member needs to register at Group manager to subscribe the group key transfer service and to establish a secret with GM. Thus, a secure channel is needed initially to share this secret with each user. Later, Group manager can send the group key and interact with all group members in a broadcast channel. Thus user repository created with group key communication with data users.

B. Data Repository Initiation

Data will be invoked based file creation and deletion basis. Group member will generate the data file based on the revocation list from the cloud. Based on the ID, Hash code template data will be created. Once the data file has been generated, data file and its template to be uploaded for secure cloud storage and retrieval of data. Thus data repository has been initiated with security template or metadata.

C. Secure Cloud Storage

The Group owner's files have been applied security. These files are stored in the cloud servers. In order to do that the cloud server have to configure using VMware tool. In cloud servers client files are stored as secured files so the crypto processes have applied. For crypto process Blowfish algorithm is used for the encryption and decryption process.

D. Secure Data Sharing

Data retrieval processes not only consist of retrieval of encrypted files from the cloud server and decrypted using respected private keys, but also the data are provided to the users based upon the authentication of the hierarchical access control of Cloud system architecture. Data or keys are revocated in the cloud frequently depending upon the kind of data owner's identity and the data to be stored on the cloud.

V. CONCLUSION

Thus the secure multi-owner data sharing scheme is achieved by the proposed scheme. It implies that any user in the group can securely share data with others by the untrusted cloud and are able to support dynamic groups efficiently. The work of the users to access the data is also easily achievable. Ultimately secured key sharing with robust authentication process results in satisfying the desired security requirements and guarantees efficiency.

REFERENCES

[1] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A. Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A View of Cloud Computing," Comm. ACM, vol. 53, no. 4, pp. 50-58, Apr. 2010.

[2] S. Kamara and K. Lauter, "Cryptographic Cloud Storage," Proc. Int'l Conf. Financial Cryptography and Data Security (FC), pp. 136- 149, Jan. 2010.

[3] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing," Proc. IEEE INFOCOM, pp. 534-542, 2010.

[4] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, "Plutus: Scalable Secure File Sharing on Untrusted Storage," Proc. USENIX Conf. File and Storage Technologies, pp. 29-42, 2003.

[5] E. Goh, H. Shacham, N. Modadugu, and D. Boneh, "Sirius: Securing Remote Untrusted Storage," Proc. Network and Distributed Systems Security Symp. (NDSS), pp. 131-145, 2003.

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, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

[6] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage," Proc. Network and Distributed Systems Security Symp. (NDSS), pp. 29-43, 2005.

[7] R. Lu, X. Lin, X. Liang, and X. Shen, "Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing," Proc. ACM Symp. Information, Computer and Comm. Security, pp. 282-292, 2010.

[8] B. Waters, "Ciphertext-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, 2008.

[9] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data," Proc. ACM Conf. Computer and Comm. Security (CCS), pp. 89-98, 2006.

[10] D. Naor, M. Naor, and J.B. Lotspiech, "Revocation and Tracing Schemes for Stateless Receivers," Proc. Ann. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO), pp. 41-62, 2001.

[11] D. Boneh and M. Franklin, "Identity-Based Encryption from the Weil Pairing," Proc. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO), pp. 213-229, 2001.

[12] D. Boneh, X. Boyen, and H. Shacham, "Short Group Signature," Proc. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO), pp. 41-55, 2004.

[13] D. Boneh, X. Boyen, and E. Goh, "Hierarchical Identity Based Encryption with Constant Size Ciphertext," Proc. Ann. Int'l Conf. Theory and Applications of Cryptographic Techniques (EUROCRYPT), pp. 440-456, 2005.

[14] C. Delerablee, P. Paillier, and D. Pointcheval, "Fully Collusion Secure Dynamic Broadcast Encryption with Constant-Size Ciphertexts or Decryption Keys," Proc. First Int'l Conf. Pairing-Based Cryptography, pp. 39-59, 2007.

[15] D. Chaum and E. van Heyst, "Group Signatures," Proc. Int'l Conf. Theory and Applications of Cryptographic Techniques (EUROCRYPT), pp. 257-265, 1991.

[16] A. Fiat and M. Naor, "Broadcast Encryption," Proc. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO), pp. 480-491, 1993.

[17] B. Wang, B. Li, and H. Li, "Knox: Privacy-Preserving Auditing for Shared Data with Large Groups in the Cloud," Proc. 10th Int'l Conf. Applied Cryptography and Network Security, pp. 507-525, 2012.

[18] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing," Proc. IEEE INFOCOM, pp. 525-533, 2010.

[19] B. Sheng and Q. Li, "Verifiable Privacy-Preserving Range Query in Two-Tiered Sensor Networks," Proc. IEEE INFOCOM, pp. 46- 50, 2008.

[20] D. Boneh, B. Lynn, and H. Shacham, "Short Signature from the Weil Pairing," Proc. Int'l Conf. Theory and Application of Cryptology and Information Security: Advances in Cryptology, pp. 514-532, 2001.