International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 3 Issue: 5 3227 – 3230

Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud

Smt. R. Anitha, Roushan Kumar, Abhishek Kumar, Shivam, Abhishek Kumar
Computer Science and Engineering,
National Institute of Engineering,
Mysore, Karnataka
India- 570008

***Abstract*—** In the present era ,cloud computing provides us a efficient way to share data amoung cloud users with low maintenance.But in multi-owner group ,there is a serious problem with preserving data and identity privacy due to frequent change of membership Some trends are opening up the period of Cloud Computing, which is an Internet-based improvement and utilize of computer technology. Security must be in given due importance for the cloud data with utmost care to the data and confidence to the data owne In this project ,we are proposing a secure multi-owner sharing scheme,for dynamic groups in the cloud.We are using group signature and encryption techniques. One of the biggest concerns with cloud data storage is that of data integrity verification at untrusted servers. To preserve data privacy, a basic solution is to encrypt data files, and then upload the encrypted data into the cloud. To resolve this problem recently the best efficient method MONA presented for secured multi owner data sharing.In our project ,we have removed the problem that occurred in existing system.In existing system whenever there is a revocation of member form group.manager has to generate a new key and then distribute to other members,this was a very tedious work,so we use a new technique of group signature so that the revoked member is not able to upload or download files. Now there is no need for generating new key each time whenever there is a revocation of members.

*****

I. INTRODUCTION

Security is one of the main element in online computing,but only security is not enough.Users can only use inline computing if they are confident enough that there data is safe. Without the assurance 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.We can take an example that any member can mislead his other team member by sharing false files or malicious files.For this we use a property called traceability, which enables the group manager to reveal the real identity of a user.As we know sharing data only by manager in a single owned manner is not flexible so we use multi-owner manner.In our project ,we mainly concerned that the secret key is not generated again and again whenever there is a revocation,We are using a revocation list which the names of the revocked members.It is helpful in a way that whenever a revocked member try to log in or uploading files ,he is not able to do these works.This is helpful in user identity proof.Now we deal with data security,only authorized member can view or upload data and there is group signature key which distributed only to the existing members of the group,it is a combination of private key of member and group key of group and private key is generated each time whenever a new member is aaded to group.Using group singnature key ,a member is able to upload or view a uploaded file. data owners store the encrypted data files in untrusted storage and distribute the corresponding decryption keys only to authorized users. Thus, unauthorized users as well as storage servers cannot learn the content of the data files because they have no knowledge of the decryption keys.

II. SYSTEM STUDY AND ANALYSIS

A. EXISTING SYSTEM

In the existing system, When there is any change in group, we need to circulate new key to every member and encrypt all the files.

As if any member is revoked then we need to redistribute the new group key to all the members present in that group,as the revoked user have the key they were using and he/she can misuse the key .

Then we have to encrypt all the files with that new key, which is quite a tedious job.

Same problem arises when we invoke any new members to the group also.

When working in cloud members feel unsafe as their identity is shown to everyone,but if it isn't then the member may misbehave as their identity is not traceable.

So we need to keep in mind that this will also not happens.

And lastly, one more problem is that there is a single data-owner in which only one can modify the files and others can only read the files.

III. PROPOSED SYSTEM

The group manager will maintain the revocation list of the members. If any of the member leave the group then the member detail is added to that list and the user will not be able to further login to that group. When the new member is added to the group then group key is provided to the member.

To remove identity privacy problem, the group manager will have the list of the uploaded files along with the *memberID* from which the file is uploaded.

By this privacy is kept secure and no one will misuse as it is traceable by the group manager.

And as it is multi-owner then any member can not only read data but also modify their own data along with the group manager. The files which are uploaded present in encrypted form , and the files can be viewed by group member as they have the group key on which he or she belongs.

IV. DESCRIPTION

In our project,we are using cryptography techniques to secure data and user private indentity for user authencation.AES algorithm is used for encrypting the data.the main conditions

 ISSN: 2321-8169
3227 – 3230

necessary for MONA projects includes any user can upload data in cloud, The encryption complexity and size of ciphertexts are independent with the number of revoked users in the system ,if any user is revocked then the whole system works asusual withut updating the private keys of other users.
The main models for MONA project are:

GROUP SIGNATURE: A group signature scheme allows any member of the group to sign messages while keeping the identity secret from verifiers. Essential to a group signature scheme is a *group manager*, who is in charge of adding group members and has the ability to reveal the original signer in the event of disputes. A group signature scheme must satisfy correctness, which ensures that honestly-generated signatures verify and trace correctly

DATA ENCRYPTION: Data encryption also allows the group manager to dynamically include new members while preserving previously computed learning the content of the stored data. In this method, they use IP multicast mechanism to shortest rekeying time to minimize adverse effect on communication. In addition, they introduce proxy mechanism for replies from group members to the group manager to reduce traffic generated by rekeying.

TRACEABILITY: an inside attacker may store and share a mendacious information to derive substantial benefit. Thus, to tackle the inside attack, the group manager should have the ability to reveal the real identities of data owners. When a data dispute occurs, the tracing operation is performed by the group manager to identify the real identity of the data owner
There are few lemmas used in our project:
Lemma 1: only authenticated user can access the cloud.
Lemma 2: Revoked users cannot access the cloud after their revocation.
Lemma 3: The revoked user is note able to access the cloud due to intraceability.

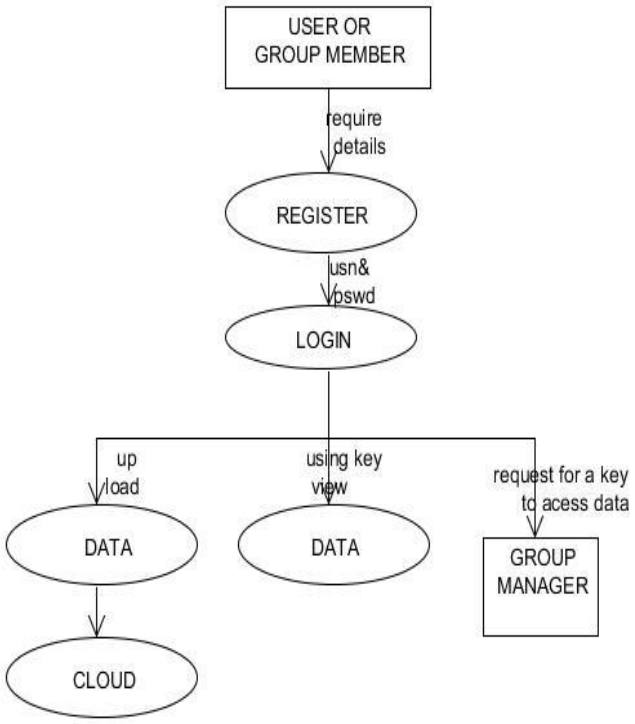
Now, we explain the system elements:
User Registration: This module is used for registering any member .Here details like name,address,email id, password,phone number,date of birth are filled. If all details about that member is correct then the member is registered.After registration a mail is generated and sent to that member mail id that the member registration is activated or not.It is responsibility of manager to add the member into any group and activation of member

Revocation List: User revocation is performed by the group manager via a public available revocation list based on which group members can encrypt their data files and ensure the confidentiality against the revoked users. In the proposed system once the user time stamp over does not wait for the group manager to update the time stamp or revocation list here once the time over the user immediately send request for extra time for access the data to the cloud.

Manager module: This module is for activating member request.When any member try to register and if all details are correct then a request is sent to manager and manager has authority to accept the request .If the request is accepted then a mail is generated and sent to the member gmail id.In that mail generated key is sent and using that key the member can view any uploaded file.This module is for login purpose of manager. Here manager name and his password is entered and if all details are correct then the manager is logged in successfully.

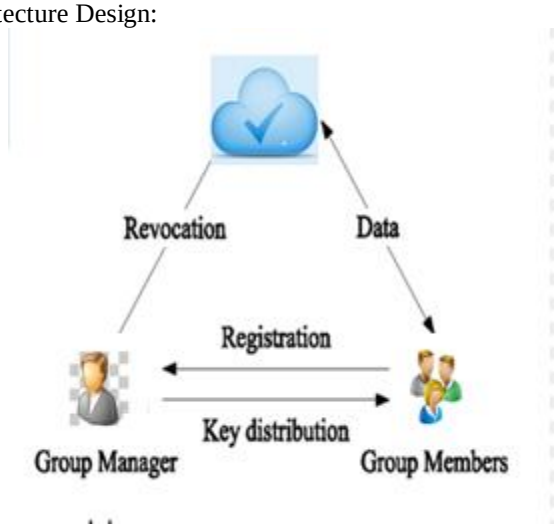
Member module: Group members are a set of registered users that will store their private data into the cloud server and Share them with others in the group. This module is used by member to upload any file.File is uploaded in encrypted way and if any member wants to view that file then they should me valid member and they have to download that file.Manager has athourity to view uploaded file so that any malicious file is not uploaded.Manager has all details about that uploaded file.

DATA FLOW: The below data flow diagram shows that under the cloud module ,there are two modulesGroup Manager module Group member module Both can login using their login details. After successful login, Group Manager activates newly added members of the cloud. He can also check the group details , file details of the cloud and he can also delete the files . After successful login, Group Member's signature is verified. After successful verification, the member can upload, download and can modify the files. The Group Member's account can be revoked after he leaves the cloud by the Group Manager. If the login fails, due to the wrong login details, both in Group Member and Group Manager modules, an error is generated. Because of which neither Manager nor Member can login. During group signature verification in the Group Member module, if the verified result turns out to be false, it is treated as an error and the Member has no access over the group.



 ISSN: 2321-8169
3227 – 3230

Architecture Design:



V. RSA ENCRYPTION ALGORITHM

RSA is one of the first practical public-key cryptosystems and is widely used for secure data transmission. In such a cryptosystem, the encryption key is public and differs from the decryption key which is kept secret. In RSA, this asymmetry is based on the practical difficulty of factoring the product of two large prime numbers, the factoring problem. RSA is made of the initial letters of the surnames of Ron Rivest, Adi Shamir and Leonard Adleman, who first publicly described the algorithm in 1977. Clifford Cocks, an English mathematician, had developed an equivalent system in 1973, but it was not declassified until 1997.

A user of RSA creates and then publishes a public key based on the two large prime numbers, along with an auxiliary value. The prime numbers must be kept secret. Anyone can use the public key to encrypt a message, but with currently published methods, if the public key is large enough, only someone with knowledge of the prime numbers can feasibly decode the message.Breaking RSA encryption is known as the RSA problem; whether it is as hard as the factoring problem remains an open challenge for the encryption key decipher.
The algorithm discussed below with an example of operations:-

- Select two large prime numbers p, q
- Compute
  $n = p \times q$
  $v = (p-1) \times (q-1)$
- Select small odd integer k relatively prime to v

gcd(k, v) = 1

- Compute d such that
  $(d \times k)\%v = (k \times d)\%v = 1$
- Public key is (k, n)
- Private key is (d, n)

- Alice and Bob would like to communicate in private
- Alice uses RSA algorithm to generate her public and private keys
  - Alice makes key (k, n) publicly available to Bob and anyone else wanting to send her private messages
- Bob uses Alice's public key (k, n) to encrypt message M:
  - compute $E(M) = (M^k)\%n$
  - Bob sends encrypted message E(M) to Alice
- Alice receives E(M) and uses private key (d, n) to decrypt it:
  - compute $D(M) = (E(M)^d)\%n$

decrypted message D(M) is original message M

- RSA algorithm for key generation
  - select two prime numbers p, q
  - compute $n = p \times q$, $v = (p-1) \times (q-1)$
  - select small odd integer k such that gcd(k, v) = 1
  - compute d such that $(d \times k)\%v = 1$
- RSA algorithm for encryption/decryption
  - encryption: compute $E(M) = (M^k)\%n$
  - decryption: compute $D(M) = (E(M)^d)\%n$
- Input: none
- Computation:
  - select two prime integers p, q
  - compute integers $n = p \times q$, $v = (p-1) \times (q-1)$
  - select small odd integer k such that gcd(k, v) = 1
  - compute integer d such that $(d \times k)\%v = 1$
- Output: n, k, and d
- Input: integers k, n, M
  - M is integer representation of plaintext message
- Computation:
  - let C be integer representation of ciphertext
    $C = (M^k)\%n$
- Output: integer C
  - ciphertext or encrypted message
- Input: integers d, n, C
  - C is integer representation of ciphertext message
- Computation:
  - let D be integer representation of decrypted ciphertext

$$D = (C^d)\%n$$

- Output: integer D
  - decrypted message

SYSTEM SPECIFICATION

 Any user in the group can store and share data files with others by the cloud. This feature of the system can be used in any MNCs for sharing data files among their employees.

 The encryption complexity and size of ciphertexts are independent with the number of revoked users in the system. In our system if a member is revoked then its effects cannot change anything. So any platform with minimum resources can deploy our system efficiently.

 A new user can directly decrypt the files stored in the cloud before his participation. If a member is new to the group the he/she can decrypt any file in the group without uploading any file.

 User revocation can be achieved without updating the private keys of the remaining users. A revocation list is maintained by the group manager using which the revoked member cannot be given access to his account.

VI. CONCLUSION

In this paper, we design a secure data sharing scheme, Mona, for dynamic groups in an untrusted cloud. In Mona, a user is able to share data with others in the group without revealing identity privacy to the cloud. Additionally, Mona supports efficient user revocation and new user joining.
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. Extensive analyses how that our proposed scheme satisfies the desired security requirements and guarantees efficiency as well.

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.
[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.*
[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.