NOVEL MULTI OWNER DATA SHARING GROUP KEY PROTOCOL

MaheshKothuru,PraveenaPothina

Abstract-- Cloud computing provides an economical and efficient solution for group resource sharing among cloud users due to the character of low maintenance. A challenging issue is sharing data in a multi-owner manner while preserving data and identity privacy from an untrusted cloud due to the dynamic nature of the membership. The proposed scheme provides privacy and complexity while handling the data sharing over cloud. To preserve data privacy, the basic solution is to encrypt data files, and then upload the encrypted data into the cloud. Unfortunately designing an efficient and secure data sharing scheme for groups in the cloud is not an easy task due to following reasons. First, the identity of the data owners must be preserved. Second, the data owner should be able to utilize all the services provided by the cloud storage service provider. Our proposed technique works with improved AES secret sharing group key mechanism and data can be uploaded to the server after the encryption of the content by using the secret group key. When a new member joined the group, new granted users can directly decrypt uploaded data files before their participation without contacting with data owners.

Keywords: AES Algorithm, Private Encryption, Round Keys.

I.Introduction

One of the primal services offered by cloud computing is data sharing. The Cloud computingis used to compute and outsource the data of organizations in cost effective and flexible manner. Data is stored in the cloud and shared among a group of users in a collaborative manner. For example, a company allows its staffs in the same group or department to store and share files such as business plans in the cloud.

Cloud storage is gaining popularity recently. In enterprise settings, we see the rise in demandfor data outsourcing, which assists in the strategic management of corporate data. It is also used as a core technology behind many online services for personal applications. Nowadays, it is easy to apply for free accounts for email, photo album, file sharing and/or remote access, with storage size more than 25 GB. Together with the current wireless technology, users can access almost all of their files and emails by a mobile phone in any corner of the world. Considering data privacy, a traditional way to ensure it is to rely on the server to enforce the access control after authentication, which means any unexpected privilege escalation will expose all data. In a shared-tenancy cloud computing environment, things become even worse.

Mahesh Kothuru, Assistant Professor, Department of CSE, GITAM University, Visakhapatnam, India, Ph No: 7382695554, mahesh.kothuru@gmail.com

Praveen Pothina, Assistant Professor, Department of CSE, GITAM University, Visakhapatnam, India, 9948283877, praveenachakravartula@gmail.com

The cloud service providers are able to deliver various services to cloud users or organizations through powerful data centers. Specifically, the cloud servers managed by cloud providers are not fully trusted by users while the data files stored in the cloud may be sensitive and confidential. The Privacy of data stored in the cloud can become compromised.

To preservedata privacy, a basic solution is to encrypting dta files, and then uploads the encrypted data into the cloud. Subsequent work focused on how dynamic data and data privacy can be supported during the public auditing process. However, most of previous work only focuses on auditing the integrity of personal data. Recently, Wangetal first designed a privacy-preserving public auditing mechanism (named Oruta) for shared data in an untrusted cloud, so that the identity of the signer on each block in shared data is not disclosed to the third party auditor (TPA) during an auditing task. By preserving identity privacy, the TPA cannot figure out which user in the group or which block in shared data is a higher valuable target.

Unfortunately, Oruta fails to scale well to a large number of users sharing data in a group. In Oruta, information used for verification are computed with ring signatures as a result, the size of verification information, as well as the time it takes to audit with it, are linearly increasing with the number of users in a group. To make matters worse, when adding new users to a group, all the existing verification information will need to be re-

computed if ring signatures are used, introducing a significant computation burden to all users. In addition, the identities of signers are unconditional protected by ring signatures, which prevent the group manager to trace the identity when someone in the group is misbehaved.

However, designing an efficient and secure data sharing scheme for groups in the cloud is not an easy task. First, the identity of the data owners must be preserved. Second, the data owner should be able to utilize all the services provided by the cloud storage service provider. Several security schemes for data sharing on untrusted servers have been proposed. These approaches have data owners storing the encrypted data files in untrusted storage and distribute the corresponding decryption keys only to authorized users.

Thus, both unauthorized users and storage servers cannot learn the content of the data files because they have no knowledge of the decryption keys. However the new data owner registration in the above said models reveals the identity of the new data owner to the others in the group. The new data owner has to take permission from other data owners in the group before generating a decrypting key.

The proposed system identified the problems during multi owner data sharing and proposed an efficient protocol and cryptographic technique for solving drawbacks in the traditional approach.

It proposed an efficient and novel secure key protocol for group key generation and using these key data owners can encrypt the files. Suppose new user register into group the user need not to contact the data owner during the downloading of files and data can be encrypted with AES before uploading the data in to the cloud.

II. Literature Review

Xuefeng Liu, Yuqing Zhang, Member, IEEE, Boyang Wang, and Jingbo Yan describedthat With the character of low maintenance, cloud computing provides an economical andefficient solution for sharing group resource among cloud users. Unfortunately, sharingdata in a multi-owner manner while preserving data and identity privacy from an untrustedcloud is still a challenging issue, due to the frequent change of the membership fordynamic groups in the cloud. By leveraging group signature and dynamic broadcastencryption techniques, any cloud user can anonymously share data with others. Meanwhile,the storage overhead and encryption computation cost of our scheme are independent withthe number of revoked users. In addition, we analyze the security of our scheme withrigorous proofs, and demonstrate the efficiency of our scheme in experiments.Moreover,the storage overhead and the encryption computation cost are constant. Extensive analyses show that our proposed scheme satisfies the desired security requirements andguarantees efficiency as well.

A.Way of Sharing

the security schemes study about several method for secure data sharing onuntrusted cloud. The only data owner or group manager has the authority to share and stored the files on untrusted cloud. Thus the data owner or group manager can send private decryption keys to the authorised users. Thus the outside users or storage server can't read the contents of the file as they are unaware of private encryption keys. Thus the complexity of the new users is increasing with no of data users and the no of revoked users respectively.only single owner group is present. The single owner manner hinders the adoption of their scheme into the case where any user is granted to store and share data .The complexities of user participation and revocation in these schemes are linearly increasing withthe number of data owners and the number of revoked users, respectively. Security is very bad.User revocation is very difficult.

The solution for preserving data privacy is to encrypt the data and then it can be stored on the cloud. Unfortunately, designing an efficient and secure data sharing scheme for groups in the cloud is not an easy task. Thusthe only data owner or group manager has the authority to share and stored the files on untrusted cloud. Thus the data owner or groupmanager can send private decryption keys to the authorised users. Thus the outside users or storage server can't read the contents of the file as they are unaware of private encryption.

III. Multi Owner Data Sharing Scheme

A secure multi-owner data sharing scheme is implies that any user in the group can securelyshare data with others by the untrusted cloud. Our proposed scheme is able to support dynamicgroups efficiently. Specifically, new granted users can directly decrypt data files uploadedbefore their participation without contacting with data owners.

User revocation can be easily achieved through a novel revocation list without updating thesecret keys of the remaining users. The size and computation overhead of encryption areconstant and independent with the number of revoked users.
A secure and privacy-preservingaccess control to users, which guarantees any member in a group to anonymously utilizethe cloud resource, is provided. Moreover, the real identities of data owners can be revealedby the group manager when disputes occur. A rigorous security analysis, and performextensive simulations to demonstrate the

efficiency of our scheme in terms of storage andcomputation overhead.

We identified the problems during multi owner data sharing and we proposed an efficientprotocol and cryptographic technique for solving drawbacks in the traditional approach. Weproposed an efficient and novel secure key protocol for group key generation and using thiskey we can encrypt the files. Suppose new user register into group the user need not to contactthe data owner during the downloading of files and data can be encrypted with AES before uploading the data in to the cloud.

A. Data owner

Data owner requires registration before uploading the data in to the service. Before the file canbe upload into the service file can be encrypted by the group key generated by group keymanager. The encryption can be done by using the AES algorithm. After encrypting the filecan be upload into server. He can download the content when ever required.

B. Group key manager

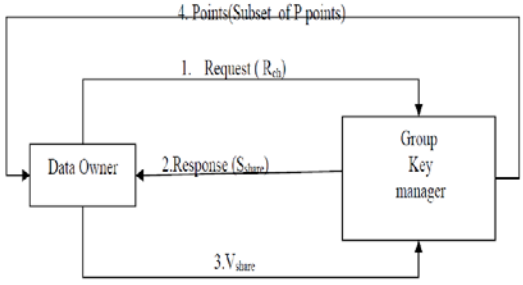
Group key manger receives the registration request from all the users, and generates averification share and forwards to all the requested users for authentication purpose, generatesthe key using key generation process and forwards the points to extraction of the key from theequation generated by the verification points.

For key generation protocol, it receives the verification shares and key as input to construct the Lagranges polynomial equation f(x), which is passed, through (0, key) and verification points,after that group key manager forwards the points to data owners. Data owners again reconstruct the key from the verification points and check the authentication code which issent by the group key manager.

When a new user tries to download the file, he need not to connect other data owner to decryption of the file, user connects to the group key manager he will update the group key anddecrypts the files with previous key again encrypt with new key and updates the new key to all the data owners Data owner initiate the request by sending the random challenge to the group key manager, as a response Group key manager sends a secret share, data owner authenticates and forwards the verification share, data owner receives the verification shares and generates the key using Lagrange's polynomial equation and forwards the points to data owners for regeneration the key.

IV. Out Sourcing of Data Over Service

Data owner reads the required file content and encrypts the file with key, which is generated by the group key manager, for encryption of the data, we use AES algorithm for encryption of the file and uploads in to the server. Data owner can download the file when ever required.

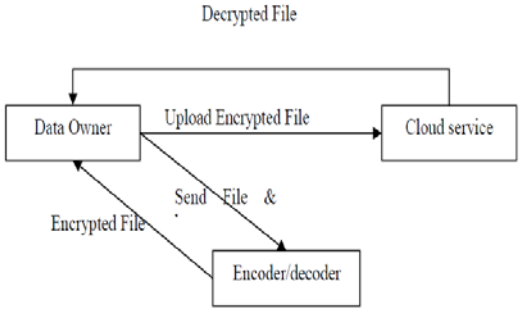


R_{ch} ----Random challenge
S_{share}---Secret share
V_{share}----verification share
$P=\{p_1,p_2 \ldots p_n\}$-------points for construction of Lagrange's equation

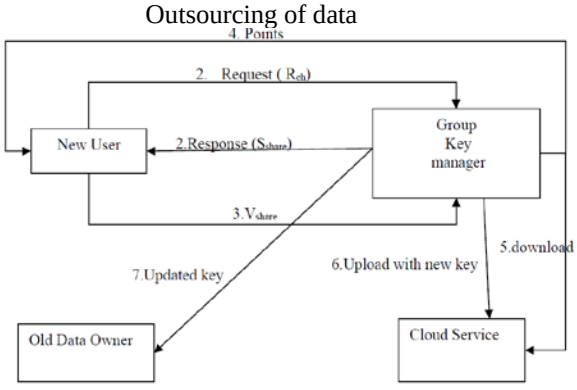
Fig.1 Initiation Process

A.User Revocation

Whenever new user tries to download the file, user need not consult the all data owners. New usercan be revoked by the group key manager in regular registration process ,Group key manager updates the key and send to all users. The key manager decrypts the file with old key and encrypts with the new key. Using the new generated points and key we can encrypt the file or decrypt file when ever required.



Outsourcing of data



Revocation of data

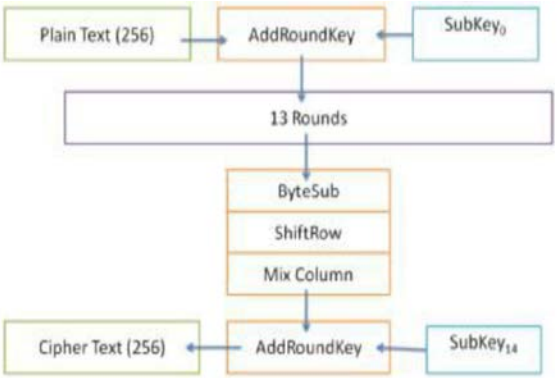
V. AES Algorithm

AES (Advanced Encryption Standard) is a symmetric encryption algorithm. The algorithm was developed by two Belgian cryptographer Joan Daemen and Vincent Rijmen. AES was designed to be efficient in both hardware and software, and supports a block length of 128 bits and key lengths of 128, 192, and 256 bits. AES has a fixed block size of 128-bits and a key size of 128, 192, or 256-bits, whereas Rijndael can be specified with any key and block sizes in a multiple of 32-bits, with a minimum of 128-bits and a maximum of 256-bits.

AES is an iterative rather than Feistel cipher. It is based on 'substitution–permutation network'. It comprises of a series of linked operations, some of which involve replacing inputs by specific outputs (substitutions) and others involve shuffling bits around (permutations). Interestingly, AES performs all its computations on bytes rather than bits. Hence, AES treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows for processing as a matrix.

Unlike DES, the number of rounds in AES is variable and depends on the length of the key. AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys.

Each of these rounds uses a different 128-bit round key, which is calculated from the original AES key. Here we use AES-256 for encryption. It is called AES-256 because it uses Plain Text and Cipher Text of 256 bits.
The design of AES-256 is shown below:



Block diagram of AES Algorithm

The key size used for an AES cipher specifies the number of repetitions of transformation roundsthat convert the plaintext, into the ciphertext. The number of cycles of repetition is 14cycles forAES-256.
Each round consists of several processing steps. They are

- Key Expansions - round keys are derived from the cipher key using Rijndael's keyschedule. AES requires a separate 128-bit round key block for each round plus one more
- Initial Round - Add Round Key to each byte of the state is combined with a block of theround key using bitwise xor.
- Rounds
  - Sub Bytes—a non-linear substitution step where each byte is replaced withanother according to a lookup table.
  - Shift Rows—a transposition step where the last three rows of the state are shiftedcyclically a certain number of steps.
  - Mix Columns—a mixing operation which operates on the columns of the state,combining the four bytes in each column.
  - Add Round Key
- Final Round (no Mix Columns)
  - Sub Bytes
  - Shift Rows
  - Add Round Key

Byte Substitution (Sub Bytes)
The 16 input bytes are substituted by looking up a fixed table (S-box) given in design. The resultis in a matrix of four rows and four columns.

Shift rows
Each of the four rows of the matrix is shifted to the left. Any entries that 'fall off' are re-insertedon the right side of row. Shift is carried out as follows −

- First row is not shifted.
- Second row is shifted one (byte) position to the left.
- Third row is shifted two positions to the left.
- Fourth row is shifted three positions to the left.
- The result is a new matrix consisting of the same 16 bytes but shifted with respect toeach other.

Mix Columns
Each column of four bytes is now transformed using a special mathematical function. Thisfunction takes as input the four bytes of one column and outputs four completely new bytes,which replace the original column. The result is another new matrix consisting of 16 new bytes. Itshould be noted that this step is not performed in the last round.

Add round key
The 16 bytes of the matrix are now considered as 128 bits and are XORed to the 128 bits of the round key. If this is the last round then the output is the ciphertext. Otherwise, the resulting 128 bits are

interpreted as 16 bytes and we begin another similar round.

AES Analysis

In present day cryptography, AES is widely adopted and supported in both hardware and software. Till date, no practical cryptanalytic attacks against AES has been discovered. Additionally, AES has built-in flexibility of key length, which allows a degree of 'future- proofing' against progress in the ability to perform exhaustive key searches. However, just as for DES, the AES security is assured only if it is correctly implemented and good key management is employed.

VI. Conclusion

In this, we developed a secure Multi owner Data sharing Group key protocol for an un-trusted cloud. In this model, a new user can store data on the cloud storage without communicating with all the data owners. The group key manager grants the key on request to the new data owners directly. The new user revocation and registration is made simple by allowing the user to communicate with the group key manager through the revocation policy.

The performance of proposed system is more compare to existing one, because in proposed system if new user enters into the cloud he does not depend on other users. The new user directly communicates with the group key manager and getting secret key. So the performance of the proposed system is high.

The security of proposed system is high compare to existing one. Since the group members only know the secret key. Suppose an unknown person enter into group he does not find the secret key the user enters into group confirm that he must be a group member.

The complexity of proposed system is low compare to existing one. Because the new user does not worry about getting the secret key i.e. the new user does not depend on the remaining group members. The new user directly communicates with group key manager and gets the secret key. The encryption and decryption of file also take less time. The storage overhead and the encryption computation cost are varied.

7. REFERENCES

1. Jingbo Yan, Boyang Wang, Yuqing Zhang, Xuefeng Liu – Secure multi-ownerdata sharing for dynamic groups in the cloud.
2. M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu,"Scalablesecure file sharing on untrusted storage.
3. S. Kamara and K. Lauter, "Cryptographic cloud storage," in Proc. of FC, January2010, pp. 136-149.
4. C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy-PreservingPublic Auditing for Secure Cloud Storage," IEEE Transactions on Computers, vol. 62.
5. Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling Public Verifiability andData Dynamic for Storage Security in Cloud Computing.