IMPLEMENTING RELIABLE AND SECURE DATA SHARING SCHEME IN THE COMMUNITY CLOUD

[1] Janarthanan R, [2] Shankari S
[1] Head of the Department, Department of Computer Science and Engineering
[2] PG Student, Department of Computer Science and Engineering
[1, 2] T.J.S. Engineering College, Chennai, India.
hodcse@tjsenggcollege.com, shankarinarayanan@gmail.com

ABSTRACT

In cloud computing, users can share data among group members with the characters of less maintenance and little management cost. Sharing data must have security guarantees, if they are out sourced. Sharing data while providing privacy preserving is still a challenging problem, when change of the membership. It might cause to the collusion attack for an un secured cloud .Data de duplication is one of the techniques which used to solve the repetition of data. The de duplication techniques are generally used in the cloud server for reducing the space of the server. To prevent the unauthorized use of data accessing and create duplicate data on cloud the encryption technique to encrypt the data before stored on cloud server. Most of the existing authentication system has certain drawbacks for that reason graphical passwords are most preferable authentication system where users click on images to authenticate themselves. Our proposed system states image based effective authentication. When the Admin uploads the file in the cloud, the admin will split the image into 4 parts. The admin will hold 2 parts and the user of that respective group can view the other 2 parts. The images are spilt randomly using pseudo random generator technique. When the user tries to download a file, the user can send the requisition to the respective admin along with the user side available 2 parts. The admin will verify both the parts and if the authentication is passed, the file will be sent to the user in an encrypted way.

Drop box is proposed for cloud storage. All files of data owners are encrypted using AES algorithm and stored in real cloud.

1.INTRODUCTION:

Cloud Computing is an innovative technology that is revolutionizing the way we do computing. The key concept of cloud computing is that you don't buy the hardware, or even the software, you need anymore, rather you rent some computational power, storage, databases, and any other resource you need by a provider according to a pay-as-you-go model, making your investment smaller and oriented to operations rather than to assets acquisition.

In the simplest terms, cloud computing means storing and accessing data and programs over the Internet instead of your computer's hard drive. The cloud is just a metaphor for the Internet. It goes back to the days of flowcharts and presentations that would represent the gigantic server-farm infrastructure of the Internet as nothing but a puffy, white cumulus cloud, accepting connections and doling out information as it floats .Hybrid services like Drop Box and Sugar Sync all say they work in the cloud because they store a synced version of your files online, but they also sync those files with local storage. Synchronization is a cornerstone of the cloud computing experience, even if you do access the file locally. CLOUD computing, with the characteristics of intrinsic data sharing and low maintenance, provides a better utilization of resources.In cloud computing, cloud service providers offer an abstraction of infinite storage space for clients to host data. It can help clients reduce their financial overhead of data managements by migrating the local managements system into cloud servers.

The main contributions of our scheme include:

We provide a secure way for key distribution without
Any secure communication channels. The users can securely obtain their private keys from group manager without any Certificate Authorities due to the verification for the public key of the user.
Our scheme can achieve fine-grained access control,
with the help of the group user list, any user in the group can use the source in the cloud and revoked users cannot access the cloud again after they are revoked.
We propose a secure data sharing scheme which
can be protected from collusion attack. The revoked users can not be able to get the original data files once they are revoked even if they conspire with the untrusted cloud. Our scheme can
achieve secure user revocation with the help of polynomial function.
Our scheme is able to support dynamic groups
efficiently, when a new user joins in the group or a user is revoked from the group, the private keys of the other users do not need to be recomputed and updated.
We provide security analysis to prove the security of our scheme. In addition, we also perform simulation to demonstrate the efficiency of our scheme.

2. PRELIMINARIES

Authority User Verification

At first Initial stage all users must create own username and password. After the Registration the user can login to their own space. This application verify the username and password which is either matched or not with the user registration form which is already created by the user while user registration process. If the valid user did not remember the username or password correctly the user can generate own password by using this application.

Image Based effective authentication

Image based password system to decrypt and encrypted the file based authentication. When the Admin uploads the file in the cloud, the admin will split the image into 4 parts. The admin will hold 2 parts and the user of that respective group can view the other 2 parts. The images are spilt randomly using pseudo random generator technique. When the user tries to download a file, the user can send the requisition to the respective admin along with the user side available 2 parts. The admin will verify both the parts and if the authentication is passed, the file will be sent to the user in an encrypted way.

Privacy-preserving

In the Privacy preservation environments, a reasonable security protocol would be developed to achieve the following requirements.
Authentication: A legal user can access its own data fields, only the authorized partial or entire data fields can be identified by the legal user, and any forged or tampered data fields cannot deceive the legal user.
Data anonymity: any irrelevant entity cannot recognize the exchanged data and communication state even it intercepts the exchanged messages via an open channel.
User privacy: any irrelevant entity cannot know or guess a user's access desire, which represents a user's interest in another user's authorized data fields. If and only if the both users have mutual interests in each other's authorized data fields, the cloud server will inform the two users to realize the access permission sharing.
Forward security: any adversary cannot correlate two communication sessions to derive the prior interrogations according to the currently captured messages.

Key distribution &Access control

Group manager takes charge of system parameters generation, user registration, and user revocation. In the practical applications, the group manager usually is the leader of the group. Therefore, we assume that the group manager is fully trusted by the other parties.
Group members (users) are a set of registered users that will store their own data into the cloud and share them with others. In the scheme, the group membership is dynamically changed, due to the new user registration and user revocation.

Once the user is revoked, The group manager creates the new encryption key for the specific group and transmits in an encrypted format using RC4 algorithm. Second the group manger updates the whole data list in the cloud server. Third the group manages updates the user list and activates the key for access.

Detect Deduplication

Data deduplication is a specialized data compression technique for eliminating duplicate copies of repeating data in storage. The technique is used to improve storage utilization and can also be applied to network data transfers to reduce the number of bytes that must be sent. Instead of keeping multiple data copies with the same content, deduplication eliminates redundant data by keeping only one physical copy and referring other redundant data to that copy. Deduplication can take place at either the file level or the block level. For file level deduplication, it eliminates duplicate copies of the same file. Deduplication can also take place at the block level, which eliminates duplicate blocks of data that occur in non-identical files.

Collusion attack

The user leaving an group are termed as revoked users. The revoked users can not be able to get the original data files once they are revoked even if they conspire with the untrusted cloud. Thus our proposed system detects the revoked users and protects the data confidentiality and privacy.

Secure data sharing

Secure data sharing is performed using private keys generated and transmitted using secure communication channels. In our scheme, the users can securely obtain their private keys from group manager Certificate Authorities and secure communication channels using RC4 algorithm.

Cloud Storage

The group user can upload the files in real cloud server named dropbox. Duplication of files are checked and the files is been uploaded in the cloud server. To get a file, the user needs to send a request to the cloud server. The cloud server will also check the user's identity before issuing the corresponding file to the user. During file access the user key has to matched by the group manager and the requested file can be downloaded by the group users.

3. EXISTING SYSTEM:

In existence private key distribution is based on the secure communication channel, In this case, which user have private key can share data unfortunately revoked user also can share data. Revoked user means who have changed their membership. Therefore, secure communication channel is a strong assumption but difficult to use. Cloud storage is not efficiently utilized. Replica of data is possible.

Disadvantage:

Existing cloud storage applications doesn't give complete data security.
Replica of data Is possible.

Extra storage consumption resulting in the extra storage cost for data application in the cloud.

4. PROPOSED SYSTEM:

The users can securely obtain their private keys from group manager. User send request to group manager for access the wanted group, at that time our system provide individual secure key to user without activation. Then group manager see the requests and activate the keys after confirm them .After user's private key gets activation, then only user can access the group. Our scheme have fine-grained access control, any user in the group can use the source in the cloud and revoked users cannot access the cloud again after they are revoked.

In our proposed system the group manager performs the below tasks when an new user joins the group or a user has left the particular group,

Update the whole user name list.

Generate a secure key and encrypt the key without activation and send to the updated user list.

Update the rights in the cloud server.

We proposed public cloud named Dropbox for data storage. Group manager makes sure that the revoked users cannot access the file if they conspire with untrusted cloud. In using advanced de-duplication system supporting authorized duplicate check. In this new de-duplication system, a hybrid cloud architecture is introduced to solve the problem

Advantage:

By integrating algorithms / techniques we can implement deduplication concepts and reduce the storage cost in a cloud for the data owners.

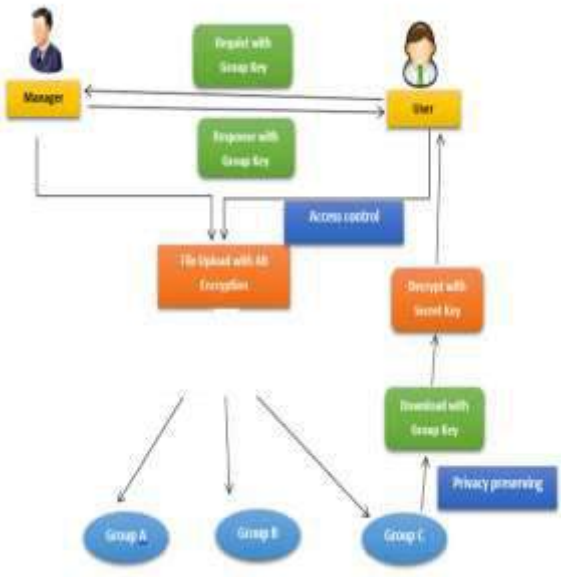
Secure protocol for anti-collusion attack.

Faster recovery and processing of data.

This would significantly decrease the processing time of load balancer.

Effective and Efficient usage of cloud Storage Space

System Architecture



5. CONCLUSION

Semantic Content Based Image Retrieval system applied to comic books. The final aim would be to provide a complete system that would be able to (1) retrieve resources similar to a query, based on the amount of mutual properties they share and the significance of these properties guided by the user relevance feedback, and explain to the user why a returned resource is considered to be relevant to the query.

6. REFERENCES

1 M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski,
G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia,
"A view of cloud computing," Commun. ACM, vol. 53, no. 4,
pp. 50–58, Apr. 2010
.

2 S. Kamara and K. Lauter, "Cryptographic cloud storage," in Proc.
Int. Conf. Financial Cryptography Data Security, Jan. 2010, pp. 136–149.

3 M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu,
"Plutus: Scalable secure file sharing on untrusted storage,"
in Proc. USENIX Conf. File Storage Technol., 2003, pp. 29–42.

4 E. Goh, H. Shacham, N. Modadugu, and D. Boneh, "Sirius: Securing
remote untrusted storage," in Proc. Netw. Distrib. Syst. Security
Symp., 2003, pp. 131–145.

5 G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved
proxy re-encryption schemes with applications to secure distributed
storage," in Proc. Netw. Distrib. Syst. Security Symp., 2005,
pp. 29–43.

6 S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable,
and fine-grained data access control in cloud computing," in Proc.
ACM Symp. Inf., Comput. Commun. Security, 2010, pp. 282–292.

7 V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based
encryption for fine-grained access control of encrypted data,"
in Proc. ACM Conf. Comput. Commun. Security, 2006, pp. 89–98.

8 R. Lu, X. Lin, X. Liang, and X. Shen, "Secure provenance: The
essential of bread and butter of data forensics in cloud
computing," in Proc. ACM Symp. Inf., Comput. Commun. Security,
2010, pp. 282–292.

Fig. 10. Comparison on computation cost of the cloud for file download among RBAC, Mona and our scheme.

9 B. Waters, "Ciphertext-policy attribute-based encryption: An
expressive, efficient, and provably secure realization," in Proc. Int.
Conf. Practice Theory Public Key Cryptography Conf. Public Key Cryptography,
2008, pp. 53–70.

10 X. Liu, Y. Zhang, B. Wang, and J. Yang, "Mona: Secure multiowner
data sharing for dynamic groups in the cloud," IEEE Trans.
Parallel Distrib. Syst., vol. 24, no. 6, pp. 1182–1191, Jun. 2013.

11 D. Boneh, X. Boyen, and E. Goh, "Hierarchical identity based
encryption with constant size ciphertext," in Proc. Annu. Int. Conf.
Theory Appl. Cryptographic Techn., 2005, pp. 440–456.

12 C. Delerablee, P. Paillier, and D. Pointcheval, "Fully collusion
secure dynamic broadcast encryption with constant-size Ci-phertexts
or decryption keys," in Proc. 1st Int. Conf. Pairing-Based Cryptography,
2007, pp. 39–59.

13 Z. Zhu, Z. Jiang, and R. Jiang, "The attack on mona: Secure multiowner
data sharing for dynamic groups in the cloud," in Proc. Int.
Conf. Inf. Sci. Cloud Comput., Dec. 7, 2013, pp. 185–189.

14 L. Zhou, V. Varadharajan, and M. Hitchens, "Achieving secure
role-based access control on encrypted data in cloud storage,"
IEEE Trans. Inf. Forensics Security, vol. 8, no. 12, pp. 1947–1960,
Dec. 2013.

15 X. Zou, Y.-S. Dai, and E. Bertino, "A practical and flexible key management mechanism for trusted collaborative computing," in Proc. IEEE Conf. Comput. Commun., 2008, pp. 1211–1219.