ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 9, September 2015

Efficient Data Sharing for Dynamic Groups in Untrusted Cloud Storage

A.Sai Kiran[1], K.Gnanendra[2]

M.Tech Student, Department of CS, Narasaraopeta Engineering College, Narasaraopeta, A.p, India[1]

Assistant Professor, Department of CSE, Narasaraopeta Engineering College, Narasaraopeta, A.p, India[2]

Abstract: The movement to cloud computing is the disruptive change in information technology. Cloud computing begin to have an effect on the modern enterprise the basic service provided by the Cloud is Data Storage Cloud computing affords a cost-effective and efficient solution for sharing group resource among cloud users with the character of low and cost effective maintenance. But the major drawback of cloud computing is sharing data in a multi-owner manner, preserving data and identity privacy from untrusted cloud storage. In this present investigation a secure multi-owner data sharing structure called as Mona, for dynamic groups in the cloud is proposed. Any cloud handler can secretly share data with others through leveraging group signature and active broadcast encryption methods. Also, the overhead storage and encryption computation cost of this scheme are self-determining with the number of revoked users. The security of the proposed scheme was analyzed and demonstrated in this study.

Keywords: Cloud computing, Privacy, Dynamic group, Data sharing.

I. INTRODUCTION

Cloud computing is typically defined as a type of computing that relies on sharing computing resources rather than having local servers or personal devices to handle applications. In cloud computing, the word cloud is used as a metaphor for "the Internet," so the phrase cloud computing means "a type of Internet-based computing," [1]where different services like servers, storage and applications are delivered to an organization's computers and devices through the internet. Cloud computing is accepted as an alternative to traditional information technology because of its fundamental resource sharing and low-maintenance characteristics. Services can be accessed from anywhere in the world by multiple devices.

The cloud model leads to basically two different kinds of clouds: private and public. The public clouds are those that offer IT services to any customer over the Internet. Private clouds offer IT services to a predefined group of customers, with access through Internet or private networks. In cloud computing, the cloud service providers (CSPs), such as Google, SAP, Oracle, etc. are providing number of services to their cloud users through powerful datacenters .Data storage is one of the supreme essential services offered by cloud.

Let us consider a practical data application. A firm allows its staffs in the same division 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. Conversely, it also poses a significant risk to the confidentiality of those stored files. 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, such as business plans. To protect data privacy, a basic solution is to encrypt data files [2], 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.

A. *Identity Privacy*

The major problem for the wide adoption of cloud computing is Identity Privacy. Cloud users may be doubtful to join cloud based computing systems without the assurance of identity privacy because if User privacy is not maintained properly then the actual identities of the user can be disclosed easily to the various kinds of intruders and cloud service providers (CSP).

B. Multiple-owner Manner

Multiple-owner manner is more flexible than single owner manner because multiple owner manners allow every member in the group should be able to alter their own data i.e. Every member able to not only read the data but also modify his part of data in the entire data file, whereas single owner manner allow only group manager to store and modify data in the cloud and members can only read the data.

C. Effect of Dynamic Groups

The groups are normally dynamic in practice joining of new staff and revocation of current employee makes the group dynamic in nature. The frequent alterations of membership make efficient and secure data sharing in Cloud very complicated and hard due to the following two primary reasons:

First, new granted users are not allowed to learn the content of data files stored before their participation by the anonymous system, because it impossible for new granted users to directly contact with anonymous data owners and get the corresponding decryption keys.

Second, to reduce the complexity of key management it is desirable to obtain an efficient membership revocation mechanism without updating the secret keys of the remaining users.

DOI 10.17148/IJARCCE.2015.4957

II.AVAILABLE SYSTEM

To preserve data privacy, a 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.

In the existing System 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. However, the complexities of user participation and revocation in these schemes are linearly increasing with the number of data owners and the number of revoked users, respectively.

Disadvantages of Existing System:

- 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.
- Only the group manager can store and modify data in the cloud
- The changes of membership make secure data sharing extremely difficult the issue of user revocation is not addressed

III. RELATED WORK

Cryptographic storage system that permits secure file sharing on un trusted servers, named Plutus [4] is proposed here. The data owner can share the file groups with others by delivering the equivalent lockbox key by dividing files into file groups and encrypting each file group with a unique file block key. However, it conveys about a heavy key distribution overhead for large-scale file sharing. Moreover, the file-block key wants to be updated and distributed again for a user revocation. File metadata and file data are the two parts in the file stored in the un trusted server [5][6]. The file metadata suggests the access control information containing a sequence of encrypted key blocks, each of which is encrypted under the public key of authorized users. Therefore, the file metadata size is proportional to the number of authorized users. The user revocation in the structure is an headstrong issue specifically for large-scale sharing, since the file metadata wants to be updated. NNL [10] construction is used for efficient key revocation in their extension. Conversely, when a new user enters the group, the private key of each user in an NNL system needs to be recomputed, which may limit the application for active groups. Additional concern is that the computation overhead of encryption linearly increases with the sharing scale. It leveraged proxy re encryptions [6] to protected distributed storage. Specifically, the data owner encrypts blocks of content with unique and symmetric content keys, which are further encrypted under a master public key. For access control [3], the server uses proxy cryptography to directly re encrypt the appropriate content key(s) from the master public key to a granted user's public key. Unfortunately, a collusion attack between the un-trusted server and any revoked malicious user can be launched, which enables them to learn the decryption keys of all the encrypted blocks. Scalable and fine-grained data admittance control scheme in cloud computing based on the KP-ABE technique is presented here. The data owner uses a random key to encrypt a file, where the random key is further encrypted with a set of attributes using KP-ABE [9]. Then, the group manager allots an access arrangement and the corresponding secret key to authorized cipher text if and only if the data file attributes satisfy the access structure. To achieve user revocation, the manager delegate's tasks of data file re encryption [13] and user secret key update to cloud servers. However, the single-owner manner may hinder the implementation of applications with the scenario, where any member in a group should be allowed to store and share data files with others.

Lu et al. [7] proposed a secure provenance scheme, which is built upon group signatures and cipher text-policy attribute-based encryption techniques. Particularly, the system in their scheme is set with a single attribute. Each user obtains two keys after the registration: a group signature key and an attribute key. Thus, any user is able to encrypt a data file using attribute-based encryption and others in the group can decrypt the encrypted data using their attribute keys. Meanwhile, the user signs encrypted data with her group signature [12][15] key for privacy preserving and traceability. However, user revocation is not supported in their scheme.

IV. PROPOSED SYSTEM

Mona, a secure multi-owner data sharing structure for active groups in the cloud to solve the challenges was presented. The main contributions of this present study contain:

1 A proposed secure multi-owner data sharing scheme. It implies that any user in the group can securely share data with others by the untrusted cloud. This scheme is able to support active groups efficiently .Specifically, new granted users can directly decrypt data files uploaded before their participation without contacting with data owners. User revocation can be easily achieved through a novel revocation list without updating the secret keys of the remaining users. The size and computation overhead of encryption are constant and independent with the number of revoked users.

2 Secure and privacy-preserving access control to users was presented here, which guarantees any member in a group to anonymously utilize the cloud resource.

3 Rigorous security analysis was provided to validate the efficiency of our structure in terms of storage and computation overhead. This was helped to solve the challenges presented above.

Figure 1 shows the flow of the system with respect to group manager and group members. it is evident that both group manager and group member have certain activities that can be performed.

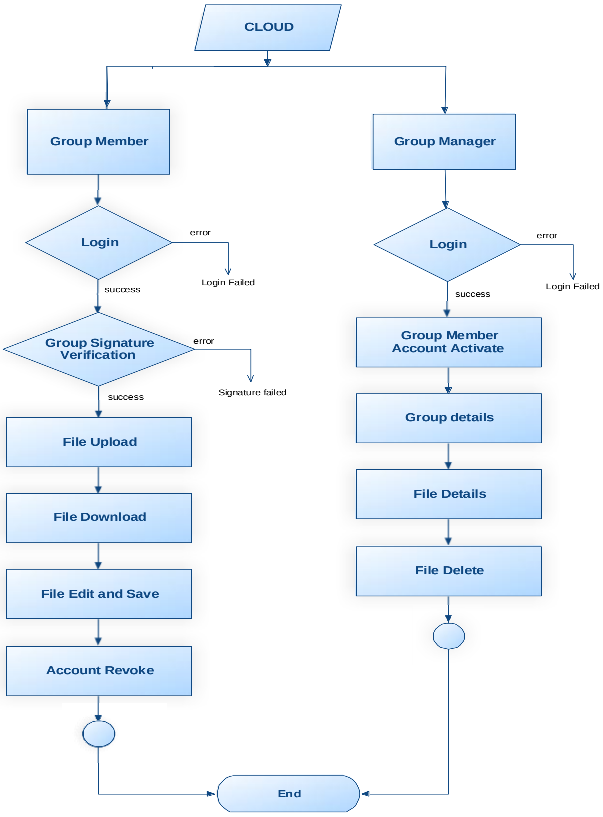


Figure 1.The flow of activities of group manager and Group member

Both users are having access to data. However, group members can gain access to the data of that group only. The multi-owner data access concept considers each member in a group as the owner (one of the owners) of data and the part of data can be manipulated by that member. The members are dynamic in nature as employees may join and leave company

V. SYSTEM MODEL AND DESIGN GOALS

The proposed system model can be explained with an example that a company uses a cloud to enable its staffs in the same group or department to share files and data.

A. *System model*

The system model contains three different entities:
- Cloud Server,
- Group manager (i.e., the company manager)
- Large number of group members (i.e., the staffs)

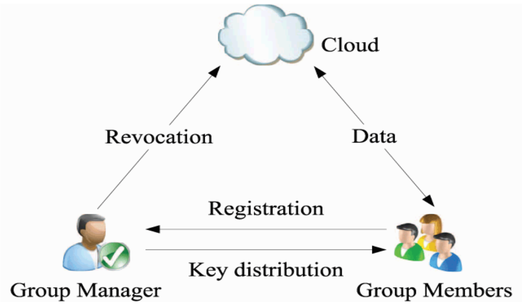


Fig.2 system model

Cloud Server is a bulky source of resources which can be distributed to its customers as a service. The cloud service providers maintain the cloud servers who are all responsible for storing complex information in the cloud and offers whenever needed. It is operated by CSPs and provides priced abundant storage services. However, the cloud is not fully trusted by users since the CSPs are very likely to be outside of the cloud users' trusted domain. Cloud server will not unkindly delete or adjust user data due to the fortification of data auditing arrangements, but will try to learn the content of the stored data and the identities of cloud users.

Group manager: is a unit which is designed for storing, sharing and managing data files stored in the cloud. Group manager is responsible for granting new users to access and increase cloud performance based on a request from them. He takes charge of system parameters generation, user registration, user revocation, and revealing the real identity of a dispute data owner. In the given example, the group manager is acted by the administrator of the company.

*Group member***:** 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. In our example, the staffs play the role of group members. Note that, the group membership is dynamically changed, due to the staff resignation and new employee participation in the company

Registration: In this module an user has to register first, then only he/she has to access the data base.

Login: In this module, any of the above mentioned person have to login, they should enter their confidential password for login.

File Upload: In this module the owner uploads the file into database, with the help of this metadata and its contents, the end user has to download the file. The uploaded file was in encrypted form, only registered user can decrypt it. Even CSP can only view the encrypted file form.

*File Download***:** The Registered users can download the file and can do updates. The modified file will be uploaded into cloud server by the user.

User Deletion: The admin can reject the user, so as that rejected user doesn't login and access the database.

B. Design Goals

In this section, we describe the main design goals of the proposed scheme including access control, data confidentiality, anonymity and traceability, and efficiency as follows

Access control: The requirement of access control is twofold. First, group members are able to use the cloud resource for data operations. Second, unauthorized users cannot access the cloud resource at any time, and revoked users will be incapable of using the cloud again once they are revoked.

DOI 10.17148/IJARCCE.2015.4957

Data confidentiality: Data confidentiality requires that unauthorized users including the cloud are incapable of learning the content of the stored data. An important and challenging issue for data confidentiality is to maintain its availability for dynamic groups. Specifically, 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

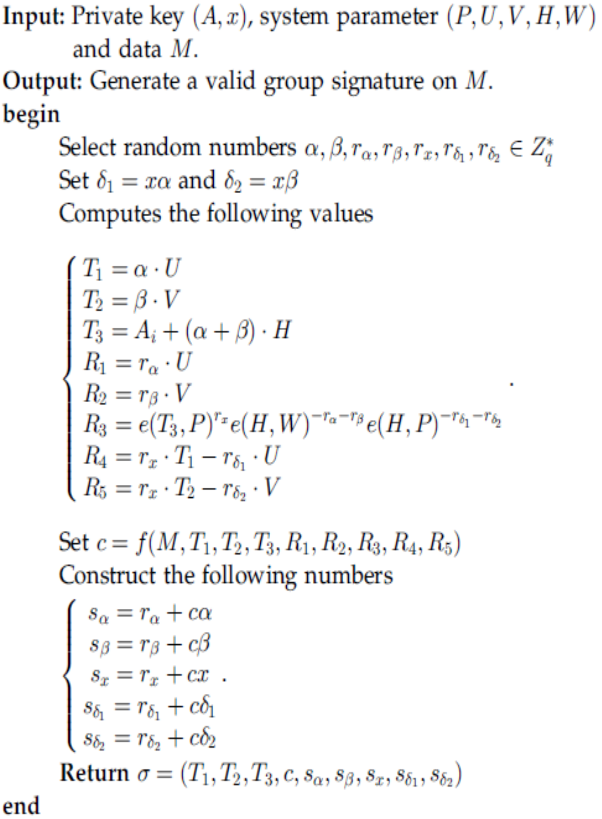
Anonymity and traceability: Anonymity guarantees that group members can access the cloud without revealing the real identity. Although anonymity represents an effective protection for user identity, it also poses a potential inside attack risk to the system. For example, an inside attacker may store 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.

Efficiency: Any group member can store and share data files with others in the group by the cloud . User revocation can be achieved without involving the remaining users. That is, the remaining users do not need to update their private keys or re encryption operations. New granted users can learn all the content data files stored before his participation without contacting with the data owner.

VI. ALGORITHMS USED

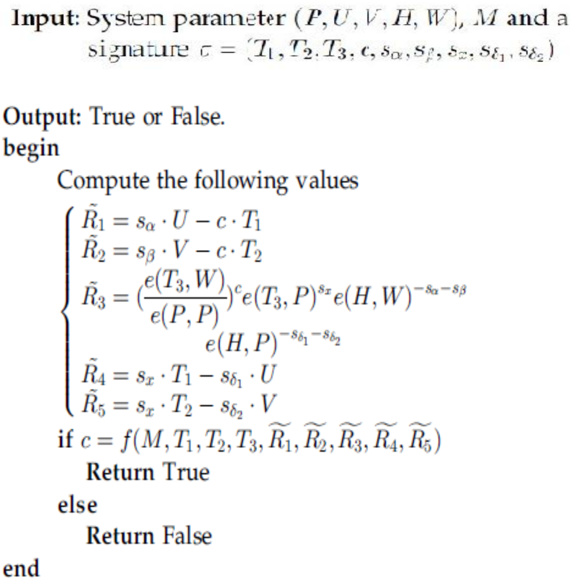
Signature generation and signature confirmation were for
The analysis.

Algorithm (1) Signature Generation



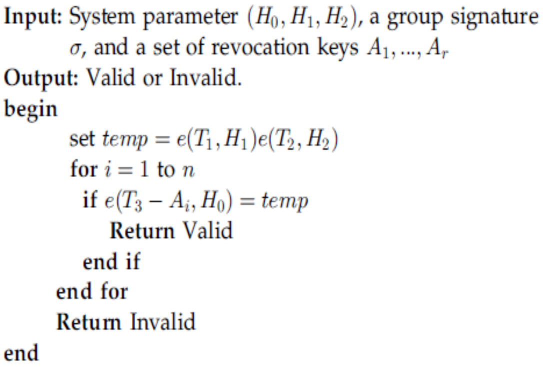
```
Input: Private key $(A, x)$, system parameter $(P, U, V, H, W)$
       and data $M$.
Output: Generate a valid group signature on $M$.
begin
    Select random numbers $\alpha, \beta, r_\alpha, r_\beta, r_x, r_{\delta_1}, r_{\delta_2} \in Z_q^*$
    Set $\delta_1 = x\alpha$ and $\delta_2 = x\beta$
    Computes the following values
    $\begin{cases} T_1 = \alpha \cdot U \\ T_2 = \beta \cdot V \\ T_3 = A_i + (\alpha + \beta) \cdot H \\ R_1 = r_\alpha \cdot U \\ R_2 = r_\beta \cdot V \\ R_3 = e(T_3, P)^{r_x} e(H, W)^{-r_\alpha - r_\beta} e(H, P)^{-r_{\delta_1} - r_{\delta_2}} \\ R_4 = r_x \cdot T_1 - r_{\delta_1} \cdot U \\ R_5 = r_x \cdot T_2 - r_{\delta_2} \cdot V \end{cases}$ .
    Set $c = f(M, T_1, T_2, T_3, R_1, R_2, R_3, R_4, R_5)$
    Construct the following numbers
    $\begin{cases} s_\alpha = r_\alpha + c\alpha \\ s_\beta = r_\beta + c\beta \\ s_x = r_x + cx \\ s_{\delta_1} = r_{\delta_1} + c\delta_1 \\ s_{\delta_2} = r_{\delta_2} + c\delta_2 \end{cases}$ .
    Return $\sigma = (T_1, T_2, T_3, c, s_\alpha, s_\beta, s_x, s_{\delta_1}, s_{\delta_2})$
end
```

Algorithm (2) Signature Verification



```
Input: System parameter $(P, U, V, H, W)$, $M$ and a
       signature $\sigma = (T_1, T_2, T_3, c, s_\alpha, s_\beta, s_x, s_{\delta_1}, s_{\delta_2})$
Output: True or False.
begin
    Compute the following values
    $\begin{cases} \tilde{R}_1 = s_\alpha \cdot U - c \cdot T_1 \\ \tilde{R}_2 = s_\beta \cdot V - c \cdot T_2 \\ \tilde{R}_3 = (\frac{e(T_3, W)}{e(P, P)})^c e(T_3, P)^{s_x} e(H, W)^{-s_\alpha - s_\beta} \\ \qquad e(H, P)^{-s_{\delta_1} - s_{\delta_2}} \\ \tilde{R}_4 = s_x \cdot T_1 - s_{\delta_1} \cdot U \\ \tilde{R}_5 = s_x \cdot T_2 - s_{\delta_2} \cdot V \end{cases}$
    if $c = f(M, T_1, T_2, T_3, \widetilde{R_1}, \widetilde{R_2}, \widetilde{R_3}, \widetilde{R_4}, \widetilde{R_5})$
        Return True
    else
        Return False
end
```

Algorithm (3) Revocation Verification



```
Input: System parameter $(H_0, H_1, H_2)$, a group signature
       $\sigma$, and a set of revocation keys $A_1, ..., A_r$
Output: Valid or Invalid.
begin
    set $temp = e(T_1, H_1)e(T_2, H_2)$
    for $i = 1$ to $n$
        if $e(T_3 - A_i, H_0) = temp$
            Return Valid
        end if
    end for
    Return Invalid
end
```

VII. CONCLUSION

In the present study, design was made for a secure data sharing structure, Mona, for active groups in an un trusted cloud. In Mona, the user can share data with others in the group without enlightening identity privacy to the cloud. Moreover, Mona supports effective user revocation and new user joining. a secure data sharing scheme,

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.

DOI 10.17148/IJARCCE.2015.4957

[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'lConf. 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'lCryptology 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.

.

DOI 10.17148/IJARCCE.2015.4957