**Secure Data Group Sharing and Conditional Dissemination with Multi-Owner in Cloud Computing**

**Abstract**:

With the rapid development of cloud services, huge volume of data is shared via cloud computing. Although cryptographic techniques have been utilized to provide data confidentiality in cloud computing, current mechanisms cannot enforce privacy concerns over ciphertext associated with multiple owners, which makes co-owners unable to appropriately control whether data disseminators can actually disseminate their data. In this paper, we propose a secure data group sharing and conditional dissemination scheme with multi-owner in cloud computing, in which data owner can share private data with a group of users via the cloud in a secure way, and data disseminator can disseminate the data to a new group of users if the attributes satisfy the access policies in the ciphertext. We further present a multiparty access control mechanism over the disseminated ciphertext, in which the data co-owners can append new access policies to the ciphertext due to their privacy preferences. Moreover, three policy aggregation strategies, including full permit, owner priority and majority permit, are provided to solve the privacy conflicts problem caused by different access policies. The security analysis and experimental results show our scheme is practical and efficient for secure data sharing with multi-owner in cloud computing.

**Index Terms**: Data sharing, cloud computing, conditional proxy re-encryption, attribute-based encryption, privacy conflict.

**Existing system:**

However, the data disseminator can disseminate all of the data owner’s data to others with this re-encryption key, which may not meet the practical requirement since the data owner may only permit the data disseminator to disseminate a particular document. A refined concept referred to as conditional PRE (CPRE) could address this issue, in which data owner can enforce re-encryption control over the initial ciphertexts and only the ciphertexts satisfying specific condition can be re-encrypted with corresponding reencryption key. However, traditional CPRE schemes only support simple keyword conditions, so they cannot match complex situations in cloud computing well. In order to support expressive conditions rather than keywords, attribute- based CPRE is proposed which deploys an access policy in the ciphertext. The re-encryption key is associated with a set of attributes, thus the proxy can reencrypt the ciphertext only when the re-encryption key matches the access policy. In this way, data owner can customize fine-grained dissemination condition for the shared data. For example, data owner allows project managers in the organization to disseminate the progress report in OneDrive, while only permits executive directors in finance department to disseminate the project budget in OneDrive during a specific time period.

**Disadvantages:**

Besides the requirement of conditional data dissemination, multiparty access control problem for data sharing in cloud computing such as cloud collaboration and cloud-based social networks comes along which means the special authorization requirements from multiple associated users can be accommodated together to control the shared data. Consider an example where a coauthoring document or a co-photo in cloud computing with three users, Alice, Bob, and Carol. If Alice who is the data owner uploads this co-authoring document or cophoto to the CSP and tags both Bob and Carol as the co-owners. Alice can restrict this data to be disseminated to a certain group of users, while the co-owners Bob and Carol may have different privacy concerns about this data. It is a massive and serious privacy problem if applying the preference of only one party, which may cause such data to be shared with undesired receivers.

**Proposed system:**

However, merging privacy preferences of data owner and multiple co-owners is not an easy task, due to privacy conflict is inevitable in multiparty authorization enforcement Privacy conflict happens when the coowners have opposite privacy policies, and it results in data being impossibly accessed with anyone. To deal with this dilemma, multiparty access control mechanisms (e.g. voting scheme) are further provided. However, all of them are based on plaintext data. In this paper, we propose an identity-based secure data group sharing and conditional dissemination scheme with multi-owner in cloud computing. To mitigate the problems mentioned above, we introduce a solution to achieve ciphertext group sharing among multiple users, and capture the core feature of multiparty authorization requirements

**Advantages:**

Multiparty access control mechanism allows the data co-owners to append new access policies to the cipher text due to their privacy preferences. Hence, the cipher text can be re-encrypted by the data disseminator only if the attributes satisfy enough access policies

The majority permit strategy, data owner can firstly choose a threshold value for data co-owners, and the cipher text can be disseminated if and only if the sum of the access policies satisfied by data disseminator’s attributes is greater than or equal to this fixed threshold.

**Architecture**

****

**Fig.** System model of proposed scheme. The user role is divided into the following categories: data owner, data co-owner, data disseminator and data accessor.

**Modules:**

**1) Trusted authority:** The trusted authority is a fully trusted part that initializes the system public key, and generates private keys as well as attribute keys for users. For example, it can be acted by the administrator of the organization or social security administration.

**2) CSP:** The CSP is a semi-trusted part that provides each user with a virtual space and convenient data storage service with the cloud infrastructure. It also appends access policies to the cipher texts for data co-owners and generates re encrypted cipher texts for users.

**3) User:** We divide the user role into the following categories: data owner, data co-owner, data disseminator and data accessor. The data owner can choose a policy aggregation strategy and define an access policy to enforce dissemination conditions. Then he encrypts data for a set of receivers, and outsources the cipher text to CSP for sharing and dissemination. The data co-owners tagged by data owner can append access policies to the encrypted data with CSP and generate the renewed cipher text. The data disseminator can access the data and also generate the re-encryption key to disseminate data owner’s data to others if he satisfies enough access policies in the cipher text. The data accessor can decrypt the initial, renewed and re-encrypted ciphertext with her or his private key.

**Software Requirements**

Operating System : Windows XP/2003 or Linux (Any OS)

User Interface : HTML, CSS

Client-side Scripting : JavaScript

Programming Language : Java

Web Applications : JDBC, Servlets, JSP

IDE/Workbench : My Eclipse 8.6

Database : Oracle 11g

Server Deployment : Tomcat 7.0

**Hardware Requirements (Minimum)**

Processor : Intel core i3 or above

Hard Disk : 500GB or more

RAM : 8GB or more

**Conclusion:**

The data security and privacy is a concern for users in cloud computing. In particular, how to enforce privacy concerns of multiple owners and protect the data confidentiality becomes a challenge. In this, we present a secure data group sharing and conditional dissemination scheme with multi-owner in cloud computing. In our scheme, the data owner could encrypt her or his private data and share it with a group of data accessors at one time in a convenient way based on IBBE technique. Meanwhile, the data owner can specify fine-grained access policy to the cipher text based on attribute-based CPRE, thus the cipher text can only be re-encrypted by Data disseminator whose attributes satisfy the access policy in the cipher text. We further present a multiparty access control mechanism over the cipher text, which allows the data co-owners to append their access policies to the cipher text. Besides, we provide three policy aggregation strategies including full permit, owner priority and majority permit to solve the problem of privacy conflicts.

**Future work**

In the future, we will enhance our scheme by supporting keyword search over the ciphertext.