# Secure and Efficient Data Sharing in Distributed Cloud Computing Environment

M Veeresha
Department of Computer Science and Engineering
Santhiram Engineering College, Nandyal, A.P.,India.

**ABSTRACT:** Today, the cloud computing became most popular and the number of users is increases day-by-day, these increases malicious, unauthorized data access and we need to employ secure accessing mechanisms using cryptographic techniques. Here, we use attribute-based mechanism to provide decryption keys to the users based on access policies provided by the owners and secure data distribution using proxy re-encryption.

**Keywords:** Cloud computing, Identity based encryption, Attribute based mechanism, proxy re-encryption, cryptographic techniques.

## 1. Introduction

Cloud Computing is the most popular phenomenon where it gains popularity due to instant access and less storage, maintenance costs. There are many cloud service providers like Amazon ,Alibaba, Google cloud, Azure etc.., that provide on-demand services to the users. The services includes storing, accessing data and resources from anywhere at any time. The main issue in these is related to security since once the data goes into the hands of Cloud Service Providers (CSP) , it is out of owners control. In order to attain privacy most of the CSP's maintains Access Control Lists(ACL), where it allows only the authorized users to access the data. But unfortunately CSP is a semi trusted party and also the data was growing tremendously from day-to- day, Due to these security concerns there is a need to provide effective solutions for data confidentiality and integrity. It is essential to adopt access control mechanisms to achieve secure data sharing in cloud computing. Currently, cryptographic mechanisms such as attribute-based encryption (ABE), identity- based broadcast encryption (IBBE), and remote attestation have been exploited to settle these security and privacy problems. ABE is one of the new cryptographic mechanisms used in cloud computing to reach secure and fine-grained data sharing. It features a mechanism that enables an access control over encrypted data using access policies and ascribed attributes among decryption keys and cipher texts. As long as the attribute set satisfies the access policy that the cipher text can be decrypted. IBBE is another prevalent technique employed in cloud computing in which users cloud share their encrypted data with multiple receivers at one time and the public key of the receiver can be regarded as any valid strings, such as unique identity and email. Hence, by using identities, data owner can share data with a group of users in a secure and efficient manner, which motivates more users to share their private data via cloud. Actually, these encryption techniques can prevent unauthorized entities from accessing the data, but it may not consider data dissemination in cloud computing. In the cloud collaboration scenario such

as Box and One Drive, the data disseminators may share the documents with new users even those outside the organization. However, once the data is encrypted with the above techniques, data disseminators are not able to modify the cipher text uploaded by data owners. Proxy re-encryption (PRE) scheme is employed to achieve secure data dissemination in cloud computing by delegating a re-encryption key associated with the new receivers to the CSP. 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 cipher texts and only the cipher texts satisfying specific condition can be re-encrypted with corresponding re encryption 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 cipher text. The re-encryption key is associated with a set of attributes, thus the proxy can re encrypt the cipher text 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.

## 2. Related Work

With the advent of rapid development of cloud computing and its uses makes it popular. These rises many securities, privacy issues on the data. Till now all the security mechanisms prevent unauthorized data access. These is further improved system that generates the appropriate encryption, decryption keys based on the access policies and attribute lists of owners and accessors. These can be achieved through attribute-based, Identity based encryption techniques, where only the accessors that satisfy all the access policies can request for the decryption key [1]. These proposed systems also provide conditional data distribution through middle-level distributors without compromising the access policies using the proxy re-encryption and conditional proxy re-encryption techniques [2].A progression of unaddressed security and protection issues develop as significant research points in cloud computing. To manage these dangers, proper encryption procedures ought to be used to ensure data secrecy. By using the Identity based method a few private data sharing plans in cloud computing[3]. In these plans, data owner redistributes encoded data to the CSP by characterizing a rundown of beneficiaries, in this way just the proposed clients in the rundown can get the decoding key and further unscramble the private data. Attribute Based Encryption (ABE) is another promising one-to-numerous cryptographic strategies to acknowledge data encryption and fine-grained get to control in cloud computing[4]. Uncommonly, ciphertext-arrangement ABE (CP-ABE) is appropriate for get to control in genuine applications because of its expressiveness in portraying the entrance approach of ciphertext proposed a privacy preserving data dispersal conspire in versatile interpersonal organizations dependent on CP- ABE[5]. Further, quality-based PRE has been utilized in cloud computing by

joining the ABE method. The intermediary can change the ciphertext under an entrance strategy into the one under another entrance approach with data disseminator's re-encryption key, and the clients who fulfill the new access arrangement can get to the plaintext. Be that as it may, the above PRE conspires just permit data spread in an all-one way. This issue is additionally tended to by Conditional PRE plot[6] , in which the intermediary can effectively re-encrypt the ciphertext just if the recommended conditions are met. Nonetheless, in prior CPRE plans the conditions are watchwords just, which would confine the adaptability while authorizing complex assignments in cloud computing[7].CPRE conspire by conveying an entrance arrangement in a ciphertext created by open key encryption. The re-encryption key is created by the mystery key related with a lot of properties, which enables the intermediary to re-encrypt the ciphertext just when these traits fulfill the entrance arrangement. proposed the main computational instrument[8]. The center thought is to evaluate thing affectability, relative significance and ability for each clashing arranging clients, and let the person who has less stringent security necessity bargain. Hu et al. proposed a deliberate way to deal with empower security safeguarding data imparting to multi-owner. This plan presents three methodologies dependent on a democratic instrument to determine the multiparty protection clashes[9]. These all just spotlights on co-owner's entrance command over plaintext data, and overlooks the data classification towards semi-trusted CSP and perniciousclients[10].

## 3. Proposed System

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 co-owners have opposite privacy policies, and it results in data being impossibly accessed with anyone. To deal with this dilemma, multiparty access control mechanisms are further provided. However, all of them are based on plaintext data. These is 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. 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.

### 3.1 Attribute-Based Encryption

Attribute-Based Encryption (ABE) is a type of public-key encryption in which the secret key of a user and the ciphertext are dependent upon attributes . In such a system, the decryption of a ciphertext is possible only if the set of attributes of the user key matches the attributes of the ciphertext. There are mainly two

types of attribute-based encryption schemes: Key-Policy Attribute-Based Encryption (KP-ABE) and Ciphertext-Policy Attribute-Based Encryption (CP-ABE). In KP-ABE, users' secret keys are generated based on an access tree that defines the privileges scope of the concerned user, and data are encrypted over a set of attributes. However, CP-ABE uses access trees to encrypt data and users' secret keys are generated over a set of attributes.

### 3.2 Identity Based Encryption

Identity-based encryption is a type of public-key encryption in which a user can generate a public key from a known unique identifier, and a trusted third-party server calculates the corresponding private key from the public key. In this way, there is no need to distribute public keys ahead of exchanging encrypted data. The sender can simply use the unique identifier of the receiver to generate a public key and encrypt the data. The receiver can generate the corresponding private key with the help of the trusted third-party server.

### 3.3 Proxy Re-Encryption

Proxy re-encryption (PRE) is a type of Public-key Encryption (PKE) that allows a proxy entity to transform or re-encrypt data from one public key to another, without having access to the underlying plaintext or private keys. Using these PRE scheme, the disseminator can disseminate all of the data to others with the help of re-encryption key. A refined concept called conditional PRE is introduced in which data owner can enforce re-encryption control over the initial ciphertexts and the cipher texts satisfying the specific conditions can be re-encrypted.

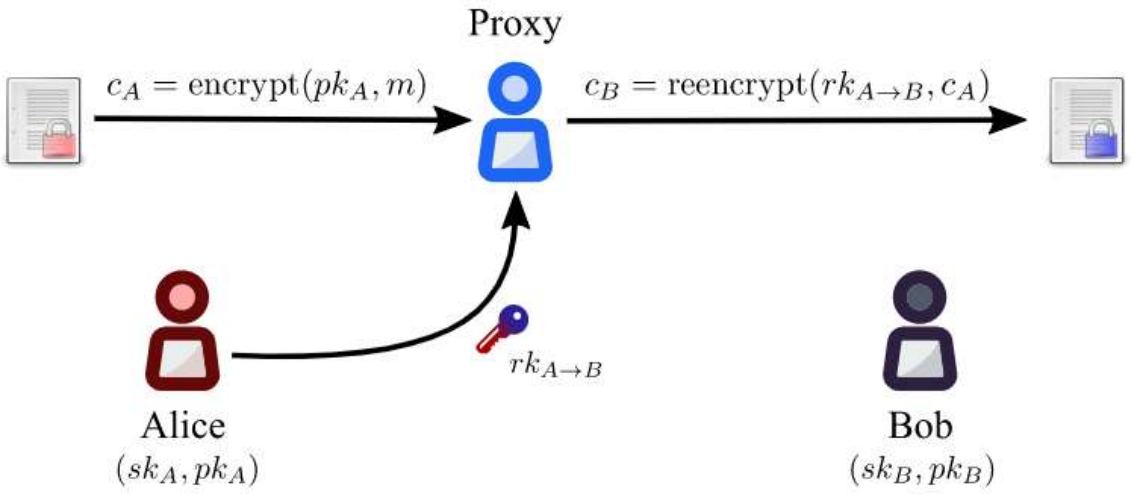


**Figure 1. Proxy Re-Encryption Process**

### 3.4 System Model

Here these papers propose a system with four modules that are data owners, data accessors, Trusted Authority, cloud service providers.

#### 3.4.1.Data Owners

Data Owner (DO)decide the access policy and encrypt the data with CP-ABE. The encrypted data will be uploaded to the Cloud Servers. DOare assumed to be honest in the system. DO's are authorized by the trusted authorities and only valid DO's are get authorized. All the authorized DO's gets encryption group key that can be used for the encrypting the data.

#### 3.4.2 Data Requester/Receivers

Data Requester/Receivers **(**DR)send the decryption request to Cloud and obtain the ciphertexts over the internet. Only when their attributes satisfy the access policies of the ciphertext, can they get access to the plaintexts. Data requester/receivers may collude to access the data that is otherwise not accessible individually.

#### 3.4.3 Cloud Servers

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 accesspoliciestotheciphertextsfordataco-ownersand Generates re-encrypted cipher text for users.

#### 3.4.4 Trusted Authority

Trusted Authority (TA) is responsible for registering users, evaluating their attributes and generating their Secret Key SKaccordingly. It runs the setupalgorithm, and issues Public Key (PK)and Master Key (MK)and it is considered as fully trusted.Here, the data is accessed only by the group to which the owner of the file belongs. Even the other groups with proper permissions of data owners can also access the data. These ensures secure group sharing by encrypting the data based on access policies and attributes. Data disseminator can disseminate the data based on the access policies specified by the data owners. All these measures can reduce the collusion of access policies of different owners and co-owners and can prevent malicious, unauthorized data access attempts.

## 4. System Study

Systems analysis is the process of examining a business situation for the purpose of developing a system solution to a problem or devising improvements to such a situation. Before the development of any system can begin, a project proposal is prepared by the users of the

potential system and/or by systems analysts and submitted to an appropriate managerial structure within the organization.

### 4.1Feasibility Study

The feasibility of the project is analyzed in this phase and business proposal is put forth with a very general plan for the project and some cost estimates. During system analysis the feasibility study of the proposed system is to be carried out. This is to ensure that the proposed system is not a burden to the company. For feasibility analysis, some understanding of the major requirements for the system is essential.

Three key considerations involved in the feasibility analysis are

- Economic Feasibility
- Technical Feasibility
- Social Feasibility

#### 4.1.1 Economic Feasibility

This study is carried out to check the economic impact that the system will have on the organization. The amount of fund that the company can pour into the research and development of the system is limited. The expenditures must be justified. Thus, the developed system as well within the budget and this was achieved because most of the technologies used are freely available. Only the customized products had to be purchased.

#### 4.1.2 Technical Feasibility

This study is carried out to check the technical feasibility, that is, the technical requirements of the system. Any system developed must not have a high demand on the available technical resources. This will lead to high demands on the available technical resources. This will lead to high demands being placed on the client. The developed system must have a modest requirement, as only minimal or null changes are required for implementing this system.

#### 4.1.3 Social Feasibility

The aspect of study is to check the level of acceptance of the system by the user. This includes the process of training the user to use the system efficiently. The user must not feel threatened by the system, instead must accept it as a necessity. The level of acceptance by the users solely depends on the methods that are employed to educate the user about the system and to make him familiar with it

## 5. Implementation and Simulation Results

These systemsare implemented using the Java programming language and JSP to develop servlet pages. The database used is MySql. JDBC is used to provide database connectivity. The results of the project can be examined by deploying code into tomcat server.

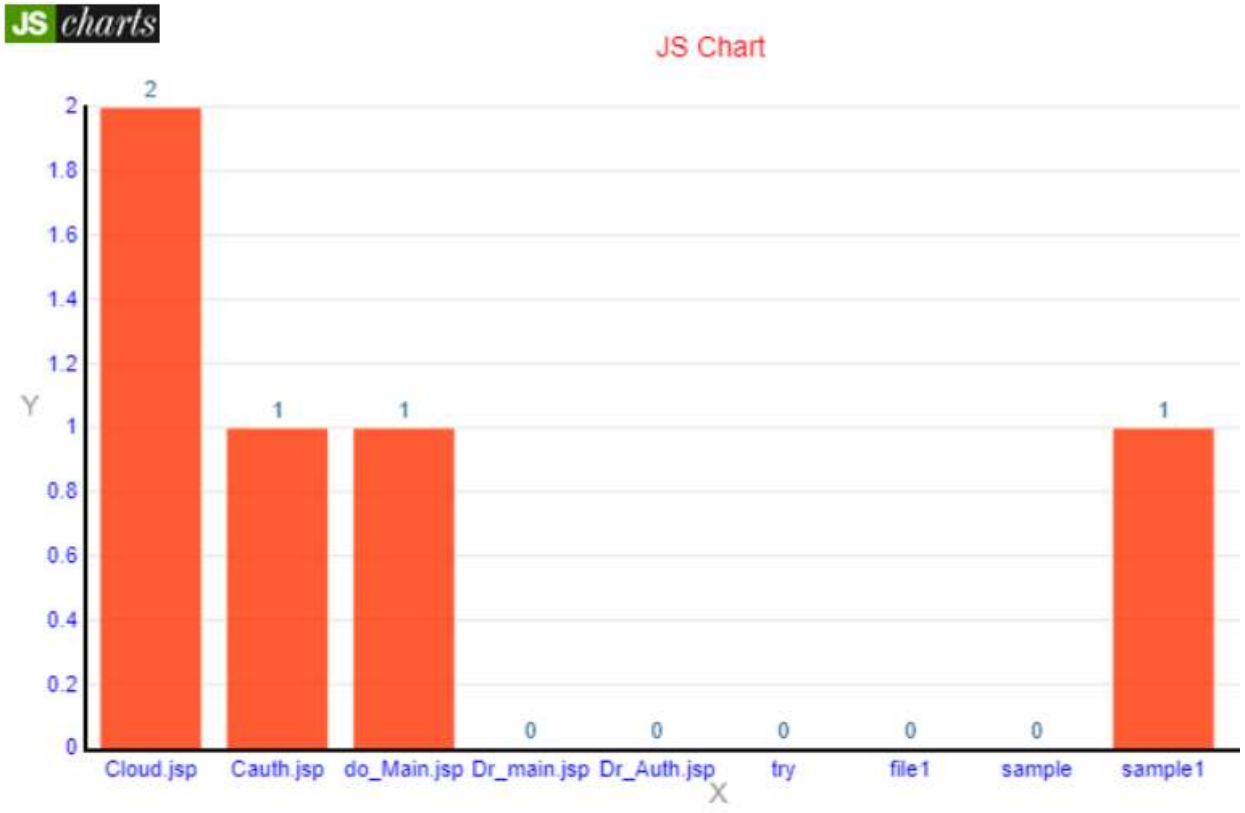


**Figure 2. File Rank Results**

Here, X-axis represents the file names and Y-axis represents the rank of the files. Here rank represents how many groups of users can download the file.Here cloud.jsp has rank 2 as it is accessed by two different group users and remaining files has either rank 1 or 0 which means the files gets accessed by the users belonging to same group or no one accessed it

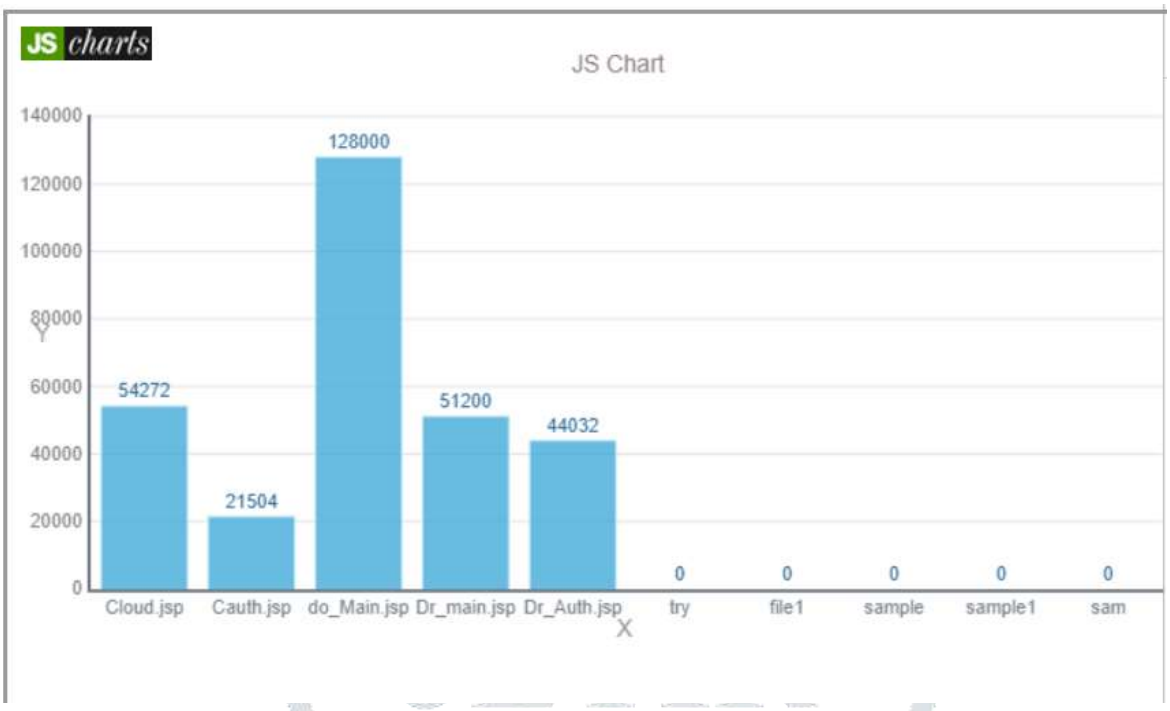


**Figure 3. Time delay results**

The above graph represents the time delay while trying to access the files. The X-axis represents the file names and Y-axis represents the time delay in milli seconds. The time delay could be of network speed. In these graph the file do_Main.jsp has more time delay compared to all other files. The reasons for these could be many like the size of the file, network speed etc.

## 6.Conclusion

The data security and privacy are 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. These challenges can be solved by this project. Here, the data owner could encrypt her or his private data and share it with a group of data accessor at one time in a convenient way based on Identity based technique. Meanwhile, the data owner can specify fine-grained access policy to the cipher text based on PRE, thus the cipher text can only be re encrypted by data disseminator whose attributes satisfy the access policy in the cipher text.

## References

**1.** Q. Zhang, L. T. Yang, and Z. Chen, "Privacy preserving deep computation model on cloud for big data feature learning," *IEEE Transactions on Computers*, vol. 65, no. 5, pp. 1351-1362, 2016.

2. H. Cui, X. Yi, and S. Nepal, "Achieving scalable access control over encrypted data for edge computing networks," *IEEE Access*, vol. 6, pp. 3049–3059, 2018.

3. K. Xue, W. Chen, W. Li, J. Hong, and P. Hong, "Combining data owner-side and cloud-side access

control for encrypted cloud storage," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 8, pp. 2062–2074, 2018.

4. C. Delerablée, "Identity-based broadcast encryption with constant size ciphertexts and private keys," *Proc. International Conf. on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2007)*, pp. 200-215, 2007.

5. N. Paladi, C. Gehrmann, and A. Michalas, "Providing user security guarantees in public infrastructure clouds," *IEEE Transactions on Cloud Computing*, vol. 5, no. 3, pp. 405-419, 2017.

6. Q. Huang, Y. Yang, and J. Fu, "Secure data group sharing and dissemination with attribute and time conditions in Public Clouds," *IEEE Transactions on Services Computing*, vol. 6, no.1, pp. 2004-2016, 2018.

7. Z. Qin, H. Xiong, S. Wu, and J. Batamuliza, "A survey of proxy reencryption for secure data sharing in cloud computing," *IEEE Transactions on Services Computing*, 2018.

8. J. Son, D. Kim, R. Hussain, and H. Oh, "Conditional proxy reencryption for secure big data group sharing in cloud environment," *Proc.* of *2014 IEEE Conference on Computer Communications Workshops*
*(INFOCOM WKSHPS)*, pp. 541–546, 2014.

9. L. Jiang, and D. Guo "Dynamic encrypted data sharing scheme based on conditional proxy broadcast re-encryption for cloud storage," *IEEE Access*, vol. 5, pp. 1336 – 1345, 2017.

10. K. Liang, M. H. Au, J. K. Liu, W. Susilo, D. S. Wong, G. Yang, Y. Yu, and A. Yang, "A secure and efficient ciphertext-policy attribute-based proxy re-encryption for cloud data sharing," *Future Generation Computer Systems*, vol. 52, pp. 95-108, 2015.