Multi-owner data sharing using attribute based encryption method in the cloud

Ms. Rupali Shelke Lecturer in Marathwada Mitra Mandal's Polytechnic, Thergaon, pune

***Abstract*— Cloud Computing is received as another option to conventional data innovation because of low maintenance attributes and its intrinsic resource sharing. In cloud computing, the service providers for example, Amazon, etc provides different services to users of cloud with the aid of intense data centers. With merging of private data management frameworks and cloud servers together. Data storage is a basic service provided by cloud system. By making use of the cloud, the cloud users can get total relief from the issues arises while storing and maintaining the local data. In particular, clients could not trust totally on the cloud servers managed by Cloud Server Company (CSP). The proposed model provides high expressiveness of access control policy, scalable user management, and less user revocation cost compared to the existing approach. I propose a secure multi-owner attribute based data sharing scheme for dynamic groups in the cloud with secure key policy. Any cloud user can continuously share data with others. The aim of paper is securely share data files in a dynamic group where multi – owner attribute authority's scheme is possible. User is able to share data files with others in the group without disturbing identity privacy to the cloud. More specially, efficient user revocation can be achieved through a public revocation list without updating or modifying the private keys of the remaining users, and new users can directly decrypt files stored in the cloud before their active participation**

I. INTRODUCTION

When Many organizations outsource their large scale data storage to the cloud to save a large amount of money. In the cloud storage service, the group members of an organization can then share data files with other group members easily by uploading their data to the cloud. In the common basic service of cloud storage safety, storage service should store data in the form of cipher text, the realization of the corresponding cloud access control service should be different with the traditional access control service model (as the access control based on role, the access control service model based on property, forcible/independent access control model, and so on). One of the most usable services offered by cloud providers is data storage. Such cloud providers cannot be trusted to protect the confidentiality of the data. Most of the time, data privacy and security issues have been major concerns for many

organizations utilizing such services. Data often encode sensitive information and should be protected as important by various organizational policies with legal regulations. Encryption is a commonly accepted approach to protect the confidentiality of the data. Encryption alone however is not sufficient as it has to enforce fine-grained access control on the data. This type of control is often based on the attributes of users, referred to as identity attributes, such as the roles of users in the organization, projects on which users are working and the database which they are using for their projects.

The revocation scheme has practical application in dynamic networks and systems. For example, when a user leaves the system, the user identity is revoked in the system which increases the security of the system. When the user is removed from the system, the authority center updates the secret key of the non-revoked user. When a user is revoked, the user's private key does not need to be updated. Comparing the two schemes, the direct revocation scheme is more suitable for open network environments. In order to prevent the revoked users from decrypting the previous cipher text, we can use the powerful computing power of cloud computing to update the cipher text when the user is revoked from the system.

In order to make the data sharing scheme of CP-ABE more applicable to practical applications, it is necessary to propose a data sharing scheme with the functions of direct revocation and keyword search. Cipher text-Policy based Encryption (CP-ABE) scheme. The existing CP-ABE scheme is not able to fulfil all security need to protect healthcare records and control of privilege revocation problem. This research paper proposes the federation based multi-Authority CP-ABE (F-CPABE) scheme for healthcare system with its subordinate strategies to outline design to healthcare records in federation-based access control scheme. The attribute revocation technique in this scheme helps to resolve both forward and backward security challenges. It has reduced attribute management overhead from a centralized system and also reduces time complexity. Servers across different security domains. Since virtualization hides the details of physical resources, the location of stored data becomes uncertain to users, which has a potential to result in mistrust of cloud storage service providers.

Compared to earlier researches, our attribute-based hierarchical file encryption scheme supports very less computation as well as storage complexity. We have constructed a new index model named data vector (DV) tree using crossover genetic algorithm which is a component of the soft computing. The DV tree is built based on the term frequency, inverse document frequency and attributes of the file. We have also developed a new key generation, encryption and decryption function for efficient retrieval of files towards the data users

II. ISSUES AND CHALLENGES

First, it is highly recommended that any member in a group should be able to fully enjoy the data storing and sharing services provided by the cloud, which is defined as the multiple-owner manner. Compared with the single owner

manner [3], where only the group manager can store and modify data in the cloud, the multiple-owner manner is more flexible in practical applications. More concretely, each user in the group is able to not only read data, but also modify his/ her part of data in the entire data file shared by the company. .Second, 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. On the other hand, unconditional identity privacy may incur the abuse of privacy. For example, a misbehaved staff can deceive others in the company by sharing false files without being traceable. Therefore, traceability, which enables the group manager (e.g., a company manager) to reveal the real identity of a user, is also highly desirable Third, Groups are normally modifiable in practical approach, e.g., new staff entered and current employee revocation in a company. The changes of membership make privacy data sharing extremely difficult by the cloud or group manager.

Fourth, It is recommended that any member in a group should be able to access the data storing and sharing by the cloud, which is shown in the multiple-owner case. Compared with the single-owner case, where only the group manager can store and edit data in the cloud, the multiple owner manner is more easily access and modify in practical applications.

Fifth, privately identification of the most significant obstacles for the wide deployment of cloud computing. Without the guarantee of identity privacy, users may be refuses to join in cloud computing systems because their real identities could be easily disclosed to cloud providers and attackers associated with that cloud.

Our contributions. To solve the challenges presented above, we propose a secure multi-owner data sharing scheme for dynamic groups in the cloud. The contributions of this paper include the following:

- A secure multi-owner data sharing scheme implies that any user in the group can securely share and modify data with others by the untrusted cloud.
- It able to support various groups efficiently and effectively for sharing and accessing data. Normally, every time new granted users can directly decrypt data files and uploaded before their participation without contacting with actual data owners. User revocation can be easily accepted list which can work without modifying the secret keys of the rest of the users. The size of the data and computation cost overhead of encryption are constant and not dependent on the number of revoked users.
- By giving secure and privacy-preserving access control to users, which can fixed any member in a group to similar utilize and access the cloud resource. Now, assigning the real identification of data owners can be opposed and cancelled by the group manager when problem occur.
- By analyzing high security, and perform extensive simulations to work for the efficiency of our scheme in terms of storage and computation overhead.

III. RELATED WORK

The contents of files placed on remote server are metadata and file data. The file metadata contains the access control data that encompass collection of encrypted keys. These metadata files are encrypted with public key of authorized users. As the file metadata should be refurbished, the user abrogation in the scheme is an uncompromising issue particularly for large-scale sharing. Nonetheless, the private key should be regenerated for each user for every new user addition into the group. This limits the application to support dynamic groups. Another issue is the encryption load enhances with the sharing scale.

The file data gives the access control information including a series of encrypted key, each of which is encrypted with the help of public key of authorized users. The user revocation is an big issue especially for large-volume sharing, since the file needs to be updated data about data that means metadata. [6] To forced security in distributed storage with privacy. Specifically the data owner encrypts blocks of data with unique and symmetric content keys. When a new user joins the group, the private key of each user in the system needs to be calculated again, which may be limited to the application for dynamic groups. The data owner encrypts content with unique and symmetric keys, which are further encrypted and further decrypted with a master public key. But, a collusion attack between the untrusted server and any revoked malicious user can be launched, which does not able to handle the decryption keys of all the encrypted blocks.

In [3], Yu et al. presented a scalable and fine-grained data accessed and shared control scheme in cloud computing based on the KPABE technique. The data owner can select any random key to encrypt a shared file, where the random key is next encrypted with a set of attributes using KPABE. Then, the group manager assign a permission for accessing structure and the corresponding secret key to authorized users, such that a user can able to decrypt a cipher text if and only if the data file attributes satisfy the access control attributes. To achieve user revocation, the manager changes various tasks of data file re encryption and user secret key edit and modify to cloud servers.

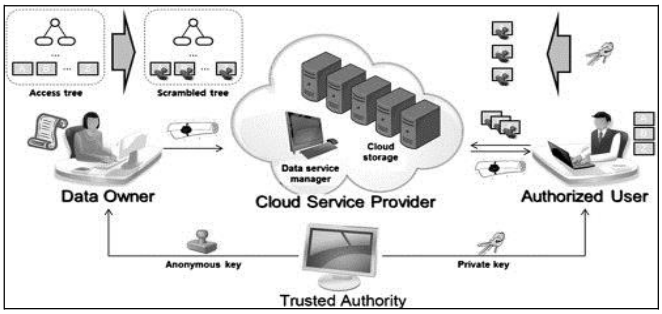
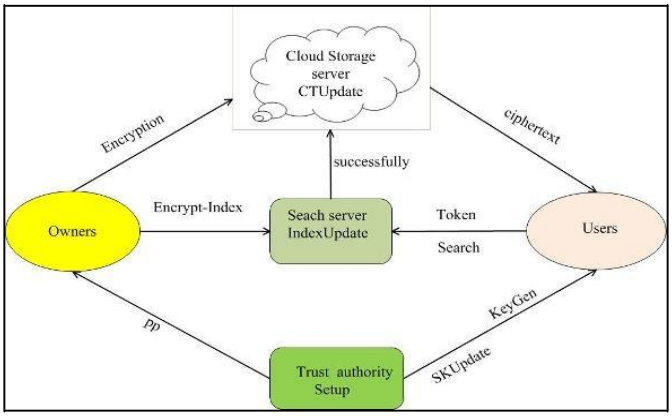


Fig 1. Attribute-Based Encryption in Cloud Storage

This paper addresses this challenging open issue by, on one hand, defining and enforcing access policies based on the attributes assign to the data, and, on the other hand, allowing the data owner to modify most of the computation tasks involved in fine-grained data access control to entrusted cloud servers without affecting the underlying data contents. We achieve this goal by exploiting and uniquely combining techniques of attribute-based encryption (ABE), proxy re-encryption, and lazy re-encryption. Our proposed scheme also has salient properties of user access privilege for data sharing, confidentiality of data and user secret key accountability. Extensive analysis shows that our proposed scheme is highly efficient and provably secures data sharing over the cloud under existing security models. Lu et al. [7] proposed a secure provisional scheme, which is built upon group signatures and cipher text-policy attribute based encryption techniques are used. Particularly, the system in their scheme is set with a single attribute. Each user obtains two keys one secrete and other public after the registration process: a group signature key and an attribute key respectively. Thus, any user is able to encrypt a shared 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 key for privacy preserving and traceability. However, user revocation does not support in their data scheme. From the above result, we can observe that How to share data files in a multiple-owner manner for dynamic groups while maintaining identity privacy from an entrusted cloud remains unchanged to be main issue. The proposed scheme uses a protocol for secure data sharing in cloud computing. Compared with the existing works the new protocol offers: The user in the group can share modify and store data files with others by the cloud. The complexity and size of shared data taken for encryption is independent with the number of revoked users in the system. User revocation can be achieved without updating or modifying the private keys of the remaining users and signed receipts will be collected after any revocation that reduces duplication of encrypted copies.

IV. PROPOSED SCHEME



Our contributions. To solve the challenges presented above, we propose Mona, a secure multi-owner data sharing scheme for dynamic groups in the cloud. The main contributions of this project include:

1. A secure multi-owner data sharing scheme implies that any user in the group can securely share data with others by the untrusted cloud.

2. It able to support dynamic 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.

3. Resource. Moreover, the Provide secure and privacy-preserving access control to users, which guarantees any member in a group to anonymously utilize the cloud real identities of data owners can be revealed by the group manager when disputes occur. 4. Provide rigorous security analysis, and perform extensive simulations to demonstrate the efficiency of our scheme in terms of storage and computation overhead We consider a cloud computing architecture by combining with an example that a company uses a cloud to enable its staffs in the same group or department to share files. The system model consists of three different entities: the cloud, a group manager (i.e., the company manager), and a large number of group members (i.e., the staffs) as illustrated in Fig. 4.

V. SYSTEM ARCHITECTURE

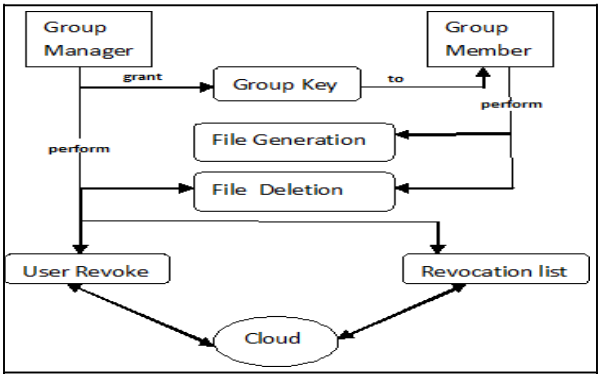


Fig 3. System Architecture

This section describes the details of system initialization, user registration, user revocation, file generation, file deletion, file access and traceability.

Registration: In this module an User has to register first with the group name , 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 login by giving their email and password.

File Upload: In this module Manager(Owner) uploads the file(along with meta data) 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 can be upload with the file name and group name

Chart Creation: User can view the chart, which is dynamically created by calculating the size of the file.

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: Manager(admin) can reject the user, so as that rejected user doesn't login and access the database.

VI. MATHEMATICAL MODEL

The signature scheme is correct in the sense that the verifier will always accept genuine signatures. This can be shown as follows:

First, if $g = h^{(p-1)/q} \bmod p$ it follows that $g^q \equiv h^{p-1} \equiv 1 \pmod p$ by Fermat's little theorem. Since $g > 1$ and q is prime, g must have order q.

The signer computes

$$s = k^{-1}(H(m) + xr) \bmod q$$

Thus

$$\begin{aligned} k &\equiv H(m)s^{-1} + xrs^{-1} \\ &\equiv H(m)w + xrw \pmod q \end{aligned}$$

Since g has order q (mod p) we have

$$\begin{aligned} g^k &\equiv g^{H(m)w} g^{xrw} \\ &\equiv g^{H(m)w} y^{rw} \\ &\equiv g^{u1} y^{u2} \pmod p \end{aligned}$$

Finally, the correctness of DSA follows from

VII. DIGITAL SIGNATURE PROCESSES

The following graphical representations of the digital signing processes.

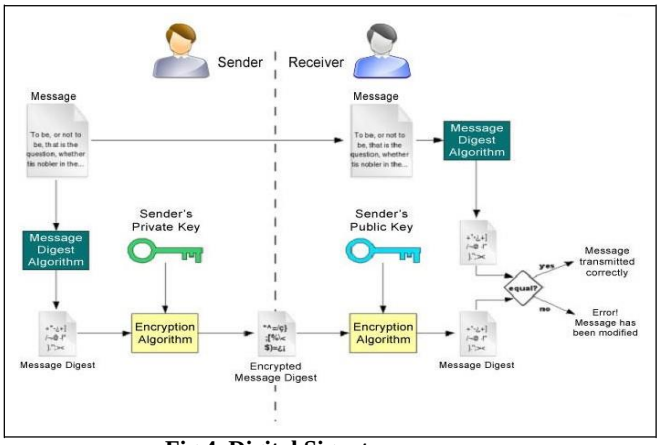


Fig 4. Digital Signature process

When a Judge gets a document digitally signed by Attorney, to verify the signature on the document, Judge's software first uses CA's (the certificate authority's) public key to check the signature on Attorney's certificate. Successful de-encryption of the certificate proves that CA created it. After the certificate is de-encrypted, Judge's software can check if Attorney is in good standing with the certificate authority and that all of the certificate information concerning Attorney's identity has not been altered (Although these steps may sound complicated, they are all handled behind the scenes by Judge's user-friendly software). Judge then signs his order digitally and a copy is electronically delivered to sheriff and court clerk in minutes. Sheriff can digitally authenticate judge's certificate and can make it available to other parties i.e. sheriff in another county if they provide proper credentials, for viewing. The digitally authenticated document provides:

- Proof of Identity.
- Prevention from unauthorized use.
- Intuitive UI for end users (encryption, decryption, and digital signatures).
- In the event that information is intercepted, encryption ensures privacy that prevents third parties from reading and or using the information.

VIII. RESULT

The proposed scheme of storage into cloud server is demonstrated using the private cloud setup with open stack. The SQL server 2005 and JAVA is used for building the ASPX pages that are used in demonstration of the proposed work.

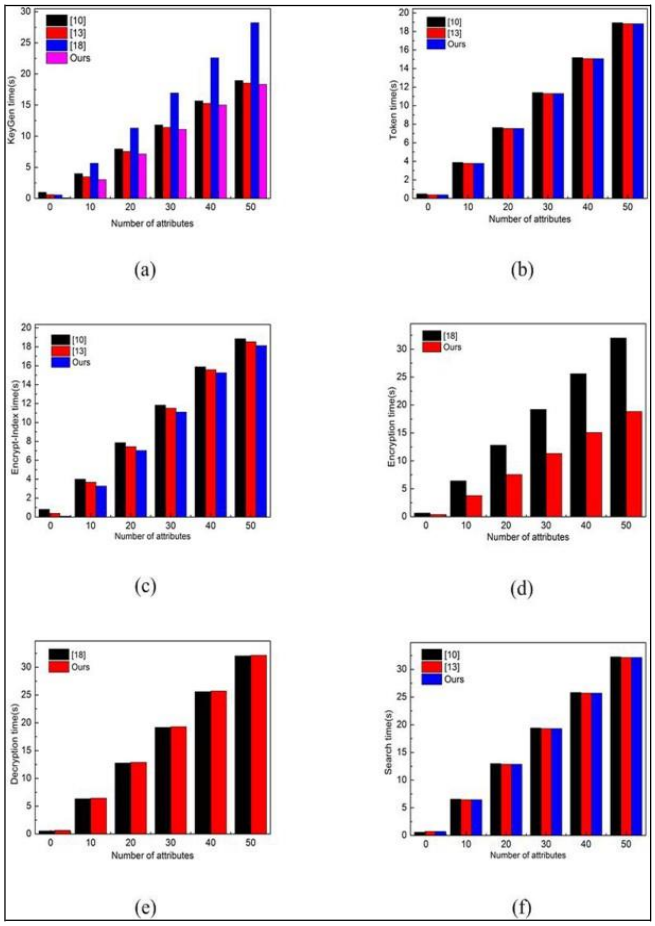


Fig 5. Experiment results on computation load

From above numerical and experimental results, we can see that our scheme exhibits an acceptable computation load if the number of attributes are carefully chosen. Actually, the computation overhead for both ECC and bilinear pairing operations can be further reduced to the magnitude of μs under hardware implementations. Moreover, as the computing power of processors is increasing rapidly, computation overload should not be a problem. What actually matters is the communication overload as bandwidth is a limited resource under environments such as wireless networks. Fortunately, the communication overload of our scheme grows linearly to the number of attributes only. Since attributes are shared by unlimited number of users, communication overload of our scheme can be well controlled even in the case of large-scale application scenarios. As a matter of fact, even in large-scale systems, the number of attributes required could be relatively small. To evaluate the performance of our scheme, we can compare it with current work. To the best of our knowledge, the only existing work that addresses the similar issue is proposed by Barth et al. In that scheme, identities of the recipients are protected by encrypting the message using every user's public key. The computational load as well as the cipher text size grow linear to the group size.

The following parameters are used to illustrate how privacy and controlled access of Data in Cloud is achieved, also addressing how the integrity and privacy of the User is achieved in the project.

- Public Key: The module generates a public key for authentication for the user to offer the user specification logging.
- File Storage: The File Storage module holds the file stored for usage by the data consumer and the files can be viewed and downloaded based on periodic time keys. Encryption: Files encrypted to give content security.
- Data Access Control: The Data Access control enables limited access to the cloud for the performance and usage of the cloud by the user.
- Data Access: The Data accessed by viewing the content of the file or downloaded for the further usage. Attribute based encryption is using data uploaded. Every node od data stored is encrypted data. Fine-Grain concept using encrypted data convert into binary value fully secure for the database.

IX. CONCLUSION

In this paper, we design a data sharing in multi-owner access control for dynamic groups in cloud. Without revealing user identity they can store and share the data efficiently in the same group. The new users can directly decrypt files stored in the cloud before their participation. Moreover, user revocation can be easily achieved through a public revocation list without updating the private keys of the remaining users. The size and Computation overhead of encryption are constant and independent with the number of revoked users. To conclude, the implementation of access policies is important in the data sharing environment. In this study, we proposed an attribute based data sharing scheme which will be implemented on a fine-grained data access control. The proposed scheme issues a key that removes key escrow. The user keys are generated by computation such that any key generation center cannot derive the private key. Thus, the proposed scheme enhances data privacy and confidentiality in the data sharing system. Therefore, the proposed scheme achieves more secure and fine-grained data access control in the data sharing system. We would like to point that the proposed scheme is efficient and scalable to securely manage user data in the data sharing system.

REFERENCES

[1] Lavanya Natarajan1 , Sujata Kulkarni2, "Data Security on Cloud Network using Key Policy Attribute Based Encryption", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 6, Issue 7, July 2017

[2] Shobha D. Patil et al, "Survey Paper On Modoc: Multi Owner Data Sharing Over Cloud" (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 6 (1) , 2017, 6-9

[3] Charanya R, Nithya S and Manikandan N, "Attribute based encryption for secure sharing of E-health data" ICSET-2017

[4] G. V. Kapse1 , Dr. V. M. Thakare2, Prof. S. S. Sherekar3 , A. V. Kapse4, "Multi-Authority Data Access Control For Cloud Storage System With Attribute-Based Encryption" National Conference on Recent Trends in Computer Science and Information Technology, (NCRTCSIT-2016)

[5] Shucheng Yu, "Data Sharing on Untrusted Storage with AttributeBased Encryption"

[6] R. Chandramouli and P. Mell, "State of security readiness," in Crossroads. ACM, 2010, pp. 23 – 25.

[7] G. Ateniese, K. Fu, M. Green, and S. Hohenberger,"Improvedproxy re-encryption schemes with applications to secure distributed storage," in Proc. of NDSS, 2005, pp. 29-43.

[8] [8] 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, 2017.

[9] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in 2007 IEEE Symposium on Security and Privacy. IEEE Computer Society, 2007, pp. 321–334.

[10] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing," Proc. IEEE INFOCOM, pp. 525-533, 2010.

[11] M. D. Chaum and E. van Heyst, "Group Signatures," in Proc Of EUROCRYPT, 1991, pp. 257-265