IOSR Journal of Engineering (IOSR JEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
PP 48-53

Security for Multi-user and Dynamic Multi-keyword Ranked Search over Cloud data

Pandit Ashok[1], Naykodi Apeksha[2], Pokharkar Shubhangi[3],
Dumbare Rajendra[4], Prof.Gholap P.S.[5]
[1](Computer, Sharadchandra Pawar College of Engineering,Dumbarwadi)[1,2,3,4]

Abstract: *Cloud computing is popular due to its feature like multiuser, multitenacy and performance. Peoples are motivated to outsource their data on cloud servers that can easily manage the data, to store data in secure form various encryption technology is used to sharing the data secularly Ciphertext-policy attribute-based encryption (CP-ABE) technology has been preferred to use. In the various fields the departments like military and healthcare having data files with multilevel hierarchy. CP-ABE hierarchy structure of shared file has not been search. In this paper, attribute-based encryption scheme an efficient file hierarchy is proposed in cloud computing. Integration of layered access structure into a singal access structure then integrated access structure is encrypted with hierarchical files.The attributes related ciphertext components could be shared by the files. Storage of cipher text and time of cost of encryption are saved. Moreover, in the assumption it is proved that proposed scheme is secure .proposed scheme is highly efficient in terms of encryption and decryption it is shown by the experimental simulations. The placed and important advantage in our scheme is that as the number of files increases our scheme is more and more usefull for this.*

Keywords: *Attribute-Based Encryption, Fine-Grained, CP-ABE*

I. Introduction

In the recent worlds network technology and mobile computing technology increases the sharing of files become more than more popular. Many social sites place the rate of sharing of information such as Facebook, MySpace, Badoo. To share such huge amount of data cloud computing is the best medium to expanding such data at the time of data sharing their is chances of leaking of data to avoid break such data security user need to encrypt their data before sharing. Access control is the first line method to control the unauthorized access to the share data.

In recent Attribute Based Encryption(ABE) has been attracted much more attention it maintained the privacy and also doing the maintenance of fine-grained, one-to-many and non-interactive access control. Cypher text-Policy Attribute based Encryption (CP-ABE) is one of the access control scheme that have much more flexibility for the general application.

In cloud computing, as illustrated in Fig. 1, authority accepts the user enrollment and creates some parameters. Cloud service provider (CSP) is act as a manager of cloud servers and that provides multiple services for client. Client can access the services through the internet anytime and anyplace. Data owner encrypts the files for security purpose and those files are uploads the generated ciphertext to CSP.if the user want to use that files then it downloads and decrypts the interested ciphertext from CSP. CSP manages all the services for client. commonly the shared files are arranged in hierarchical structure approach. That is, the group of files are distributed level by level and group containing different access levels. If the files with same access structure can be encrypted in a group, by using this scheme the storage cost of ciphertext and time cost of encryption could be saved.

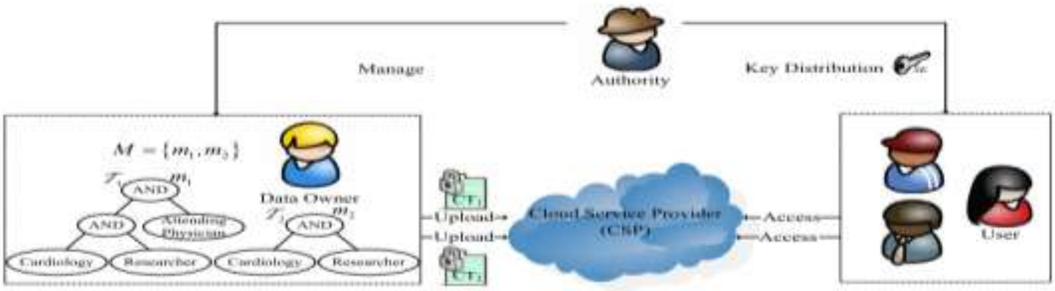

Fig.1 An Example Of Secure Data Sharing In Cloud Computing.

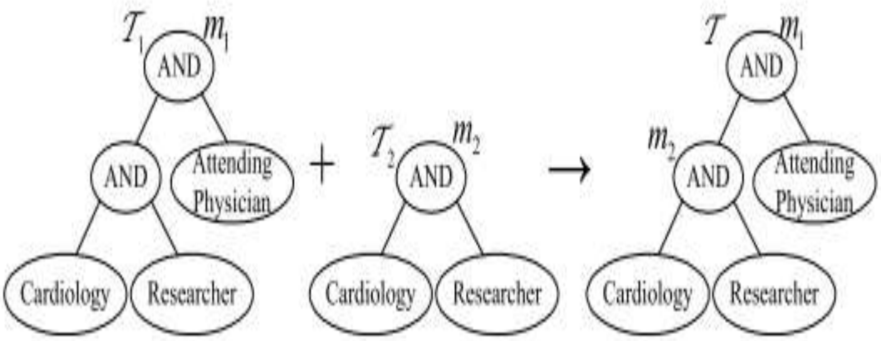

Fig.2. The Integrated Access Structure. T1 and T2 access structures of m1 and m2, respectively .T is the Integrated access structure of m1 and m2.

Here let us take the personal health record (PHR) for example . To securely share the PHR information in cloud computing, a patient divides his PHR information M into two parts: personal information m1 that may contain the patient’s name, social security number, telephone number, home address, etc. The medical record m2 which does not contain sensitive personal information, such as medical test results, treatment protocols, and operation notes. Then the patient adopts CP-ABE scheme to encrypt the informationm1 and m2 by different access policies based on the actual need. For example, an attending physician needs to access both the patient’s name and his medical record in order to make a diagnosis, and medical researcher only needs to access some medical test results for academic purpose in the related area, where a doctor must be a medical re searcher ,and the converse is not necessarily true. Suppose that the patient sets the access structure of m1 as: T1 {(“Cardiology” AND “Researcher”) AND “Attending Physician”}. Similarly,m2 is termed as: T2 {“Cardiology” AND “Researcher”}. The example is deployed in cloud system as shown in Fig. 1.Apparently, the information needs to be encrypted twice ifm1 and m2 are encrypted with access structures T1 and T2,respectively. Two ciphertexts CT1 = {T1, C ˜1, C1, ∀y ∈ Y1 :Cy, Cy } where Y1={“Cardiology”, “Researcher”, “Attending Physician”} and CT2 = {T2, C ˜2, C2, ∀y ∈ Y2 : Cy, Cy } where={“Cardiology”, “Researcher”} will be produced [11].In the Fig. 1, we can find that the two access structures have hierarchical relationships where the access structure T1is the extension of T2 . The two structures could be integrated into one structure T as shown in Fig. 2. If the two files could be encrypted with the integrated access structure and produce ciphertext CT = {T , C ˜, C, ∀y ∈ Y : Cy, Cy }where Y={“Cardiology”, “Researcher”, “Attending Physician”}. Here, the components of ciphertext {T , Cy, Cy } are related to policy. Meanwhile, access structure could be shared by the two files. Therefore, the computation complexity of encryption and storage overhead of ciphertext can be reduced greatly. Moreover, since transport nodes (refer to Fig. 3below) are added in the access structure, users can decrypt all authorization files with computation of secret key once. The computation cost of decryption can also be reduced if users need to decrypt multiple files at the same time.

show that FH-CP-ABE has low storage cost and computation complexity in terms of encryption and decryption. It should be noticed that the proposed scheme differs from

the subsequent CP-ABE schemes , which utilize the user layered model to distribute the work of key creation on multiple domain authorizations and lighten the burden of key authority center. In addition, the part of this work is presented in. The work presented in that conference paper is rough and incomplete, where some important aspects haven’t been considered.

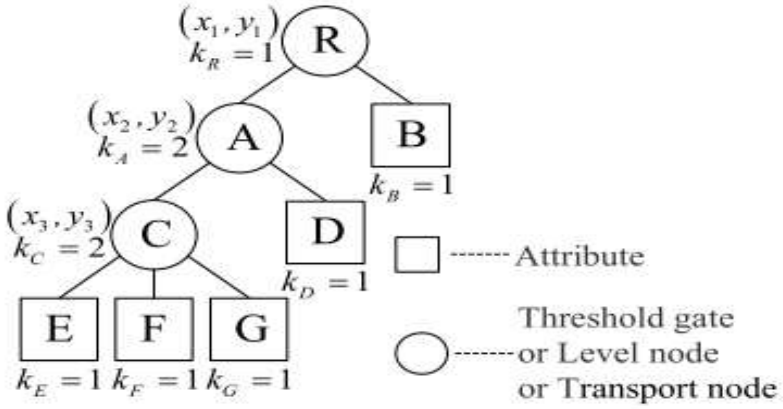

Fig.3. An example of three-level access tree.

II. Litrature Survaey

1. Ciphertext-Policy Hierarchical Attribute-based Encryption for Fine-Grained Access Control of Encryption Data :-

ciphertext-policy attribute based encryption (CPABE) scheme is based on, a private key holder is related with a set of attributes while the data is encrypted under an access structure defined by the data provider. In most proposed schemes, the characteristics of the attributes are treated as same level. In recent real world , the attributes are always in the different levels. In this paper, under a different hierarchy of attributes the scheme is proposed with the name of ciphertext-policy hierarchical attribute based encryption. The CP-HABE scheme is proved to be secure under the decisional q-parallel bilinear Diffie-Hellman exponent assumption, which can be considered as the generalization of the traditional CP-ABE.

In this paper, we propose a scheme called ciphertext policy hierarchical attribute based encryption in which the attributes in the system are not always in the same level. We present specific construction of CP-HABE which uses the hierarchical access structure that can be considered as a generalization of traditional ABE. Only when a set of attributes possessed by the user satisfies the hierarchical access structure can he/she decrypt the ciphertext. We also give a security model for CP-HABE. Finally, we prove our scheme under the security model by reducing it to decisional q-parallel bilinear Diffie-Hellman exponent assumption. More importantly, this construction can exhibit significant improvement over the traditional ABE schemes accordant with the practical situation.

2. Extended Proxy-Assisted Approach: Achieving Revocable Fine-Grained Encryption of Cloud Data :-

The potential provided by theAttribute-based encryption to be deployed in a cloud computing environment to provide scalable and fine-grained data sharing. However, user Abolishwithin Attribute-Base-Encryption deployment remains a challenging issue to overcome, particularly when there is a large number of users. In this paper, extended proxy-assisted approach is introduced, which weakens the trust required of the cloud server. Based on cloud server from colluding with a third party to hinder the user revocation functionality. We present the utility of our approach by making a construction of the proposed approach, designed to provide efficient cloud data sharing and user revocation. A way is implemented to demonstrate the practicality of our proposed construction.

In this paper, we presented an extended proxy-assisted approach in order to overcome the limitation of needing to trust the cloud server not to disclose users' proxy keys inherent in proxy/mediator assisted user revocation approaches. In our approach, we bind the cloud server's private key to the data decryption operation, which requires the cloud server to reveal its private key should the cloud server decide to collude with revoked users. We then formulated a primitive, 'revocable cloud data encryption', under the approach. We presented a concrete construction of the primitive and implemented the construction using a proof-of-concept. The experimental results suggested that our construction is suitable for deployment even on smart mobile devices.

3. Secure sharing of personal health records in cloud computing: Ciphertext-policy attribute-based encryption :-

Online personal health record (PHR) enables patients to manage their own medical records in a centralized way, which greatly facilitates the storage, access and sharing of personal health data. With the emergence of cloud computing, it is attractive for the PHR service providers to shift their PHR applications and storage into the cloud, in order to enjoy the elastic resources and reduce the operational cost. However, the patients lose physical control to their personal health data by by storing PHRs in the cloud, which makes it necessary for each patient to encrypt her PHR data before uploading to the cloud servers. In the encryption, it is difficult to achieve fine-grained access control to PHR data in a scalable and efficient way to control. For each patient, if the number of users having access then the PHR data should be encrypted so that it is scalable to all the user. Also, since there are multiple owners (patients) in a PHR system and every owner would encrypt her PHR files using a different set of cryptographic keys, it is important to reduce the key distribution complexity in such multi-owner settings. Existing cryptographic enforced access control schemes are mostly designed for the single-owner scenarios.

In this paper, we propose a novel framework for access control to PHRs within cloud computing environment. To enable fine-grained and scalable access control for PHRs, we leverage attribute based encryption (ABE) techniques to encrypt each patients' PHR data. To reduce the key distribution complexity, we divide the system into multiple security domains, where each domain manages only a subset of the users. In this way, each patient has full control over her own privacy, and the key management complexity is reduced dramatically. Our proposed scheme is also flexible, in that it supports efficient and on-demand revocation of user access rights, and break-glass access under emergency scenarios.

4.Hierarchical attribute-based encryption for fine-grained access control in cloud storage services :-

Cloud computing, as an emerging computing paradigm, enables users to remotely store their data into a cloud so as to enjoy scalable services on-demand. Especially for small and medium-sized enterprises with limited budgets, they can achieve cost savings and productivity enhancements by using cloud-based services to manage projects, to make collaborations, and the like. However, allowing cloud service providers (CSPs), which are not in the same trusted domains as enterprise users, to take care of confidential data, may raise potential security and privacy issues. To keep the sensitive user data confidential against untrusted CSPs, a natural way is to apply cryptographic approaches, by disclosing decryption keys only to authorized users. However, when enterprise users outsource confidential data for sharing on cloud servers, the adopted encryption system should not only support fine-grained access control, but also provide high performance, full delegation, andscalability, so as to best serve the needs of accessing data anytime and anywhere, delegating within enterprises, and achieving a dynamic set of users. In this paper, we propose a scheme to help enterprises to efficiently share confidential data on cloud servers. We achieve this goal by first combining the hierarchical identity-based encryption (HIBE) system and the ciphertext-policy attribute-based encryption (CP-ABE) system, and then making a performance-expressivity tradeoff, finally applying proxy re-encryption and lazy re-encryption to our scheme.

In this paper, we construct a scheme, which has several traits: (1) high performance; (2) fine-grained access control; (3) scalability; (4) full delegation. Our HABE scheme, which is also collusion resistant, can be proven to be semantically secure against adaptive chosen plaintext attacks under the BDH assumption and the random oracle model.

5. An efficient ciphertext-policy attribute-based access control towards revocation in cloud computing :-

It is secure for customers to store and share their sensitive data in the cryptographic cloud storage. However, the revocation operation is a sure performance killer in the cryptographic access control system. To optimize the revocation procedure, we present a new efficient revocation scheme which is efficient, secure, and unassisted. In this scheme, the original data are first divided into a number of slices, and then published to the cloud storage. When a revocation occurs, the data owner needs only to retrieve one slice, and re-encrypt and re-publish it. Thus, the revocation process is accelerated by affecting only one slice instead of the whole data. We have applied the efficient revocation scheme to the ciphertext-policy attribute-based encryption (CP-ABE) based cryptographic cloud storage. The security analysis shows that our scheme is computationally secure. The theoretically evaluated andexperimentally measured performance results show that the efficient revocation scheme can reduce the data owner's workload if the revocation occurs frequently.

To presented the first revocation scheme which is efficient, secure, and unassisted. The scheme can promote the usage of cryptographic cloud storage by reducing DO's workload. We described how to apply the efficient scheme to a CP-ABE based cryptographicaccess control system, and evaluated its security and performance. The evaluated results show that the efficient revocation scheme is computationally secure, and its revoking performance is better than that of the complete scheme if the revocation occurs frequently. Measured performance shows that DO will benefit from the efficient revocation scheme if the average number of revocations is greater than 0.462. In summary, the efficient revocation scheme provides an optimal tradeoff in terms of security and efficiency.

III. Project Background

Sahai and Waters proposed fuzzy Identity-Based Encryption (IBE) in 2005, which was the prototype of ABE. Latterly, a variant of ABE named CP-ABE, was proposed.• In CP-ABE scheme, user's key SK is described by an attribute set S while ciphertext CT is produced by encrypting plaintext M with an access policy T .If data owner shares k files, i.e., M = {m1,. . ., mk},with same access policy T in the cloud, the files M = {m1,. . .,mk} can be encrypted and generated CT = {T , C ˜ = Me(g, g)αs, C = hs, ∀y ∈ Y :Cy = gqy(0), Cy = H(att(y))qy(0)} by using the typical CP-ABE scheme [11]. If the k files M = {m1,. . ., mk}have different access policies T = {T1,. . ., Tk} in the cloud, the files can be encrypted individually, and created ciphertext CT = {CT1,. . . , CTk} by running CP-ABE scheme , where CTi = {Ti, C ˜ = mie(g, g)αs,C, ∀y ∈ Y : Cy, Cy }. During the decryption, user can decrypt the ciphertext CTi if and only if there is a "match" between the attributes set S and access structure Ti. Since Gentry and Silverberg proposed the first notion of hierarchical encryption scheme, many hierarchical CP-ABE schemes have been proposed. For example, Wang et al. proposed a hierarchical ABE scheme by combining the hierarchical IBE and CP-ABE. Wan et al. proposed hierarchical ABE scheme. Later, Zou gave a hierarchical ABE scheme, while the length of secret key is linear with the order of the attribute set. A ciphertext policy hierarchical ABE scheme with short ciphertext is also studied in . In these schemes, the parent authorization domain governs its child authorization domains and a top-level authorization domain creates secret key of the next-level domain. The work of key creation is distributed on multiple authorization domains and the burden of key authority center is lightened. At present, there are three types of access structures AND gate, access tree, and linear secret sharing scheme (LSSS) used in existing CP-ABE schemes. Cheung and Newport first used AND gate access structure to achieve CP-ABE scheme. Later, some improved schemes are proposed. Meanwhile, there are CP-ABE schemes based on access tree that support AND, OR, and threshold, and based on LSSS where and are the typical schemes of access tree and LSSS.

IV. Motivation

With the increasing of network technology and mobile terminal, online data sharing has become a new "pet", such as Facebook, Myspace, and Badoo. Meanwhile, cloud computing is one of the most capable application platforms to solve the unstable increasing of data sharing. In cloud computing, to keep data from leaking, users require to encrypt their data before being shared. Access control is controlling as it is the first line of security that avoid unauthorized access to the shared data. Recently, attribute-based encryption (ABE) has been interested much more attentions since it can save data privacy and gathers fine-grained, one-to-many, and non-interactive access control. Cipher text-policy attribute based encryption (CP-ABE) is one of appropriate method which has much more adjust ability and is more applicable for generic applications.

V. Architecture System

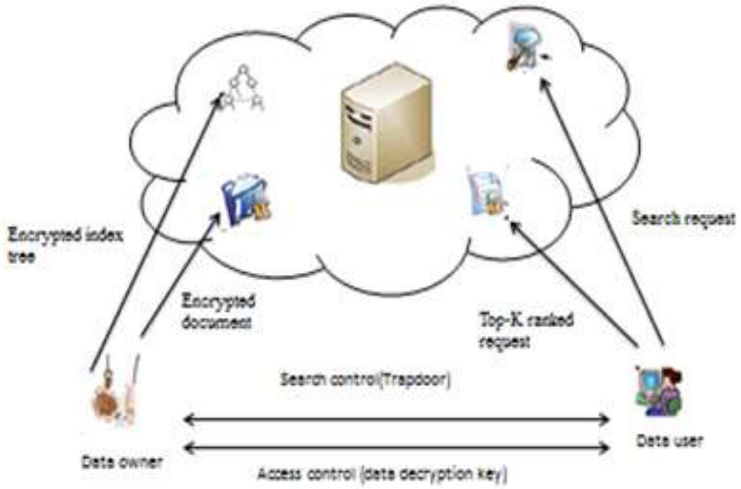

Fig. Architecture of System

VI. Advantage

- Authentication of clients who store and change information on cloud.
- Only authorized users can access the data.
- Data is stored in Encrypted format.
- Multi-Level keyword search.
- Encryption of media files is done.
- Access provided to the authorized user who have keyword to decrypt the encrypted file.

References

[1]. C.-K. Chu, W.-T.Zhu, J. Han, J.-K. Liu, J. Xu, and J. Zhou, "Security concerns in popular cloud storage services," IEEE Pervasive Comput., vol. 12, no. 4, pp. 50–57, Oct./Dec. 2013.

[2]. T. Jiang, X. Chen, J. Li, D. S. Wong, J. Ma, and J. Liu, "TIMER: Secure and reliable cloud storage against data re-outsourcing," in Proc. 10th Int.Conf. Inf. Secur. Pract.Exper., vol. 8434. May 2014, pp. 346–358.

[3]. [3] K. Liang, J. K. Liu, D. S. Wong, and W. Susilo, "An efficient cloudbased revocable identity-based proxy re-encryption scheme for public clouds data sharing," in Proc. 19th Eur. Symp. Res. Comput. Secur.,vol. 8712. Sep. 2014,pp.257–272.

[4]. T. H. Yuen, Y. Zhang, S. M. Yiu, and J. K. Liu, "Identity-based encryption with post-challenge auxiliary inputs for secure cloud applications and sensor networks," in Proc. 19th Eur. Symp. Res. Comput. Secur.,vol. 8712. Sep. 2014, pp. 130–147.

[5]. K. Liang et al., "A DFA-based functional proxy re-encryption scheme for secure public cloud data sharing," IEEE Trans. Inf. Forensics Security, vol. 9, no. 10, pp. 1667–1680,Oct.2014.

[6]. T. H. Yuen, J. K. Liu, M. H. Au, X. Huang, W. Susilo, and J. Zhou, "k-times attribute-based anonymous access control for cloud computing," IEEE Trans. Comput., vol. 64, no. 9, pp. 2595–2608, Sep. 2015.

[7]. J. K. Liu, M. H. Au, X. Huang, R. Lu, and J. Li, "Fine-grained two factor access control for Web-based cloud computing services," IEEE Trans. Inf. Forensics Security, vol. 11, no. 3, pp. 484–497, Mar. 2016.

[8]. Sahai and B. Waters, "Fuzzy identity-based encryption," in Advances in Cryptology. Berlin, Germany: Springer, May 2005, pp. 457–473.

[9]. V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Proc. 13th ACM Conf. Comput. Commun.Secur., Oct. 2006, pp. 89–98.

[10]. W. Zhu, J. Yu, T. Wang, P. Zhang, and W. Xie, "Efficient attribute-based encryption from R-LWE," Chin. J. Electron., vol. 23, no. 4, pp. 778–782, Oct. 2014.