International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 04 | Apr-2018 www.irjet.net p-ISSN: 2395-0072

A Review Paper on an Efficient File Hierarchy Attribute Based Encryption Scheme in Cloud Computing

Shital Panchal[1], Kamthane A.N.[2], Shital Gaikwad[3]

[1]*P.G. Student, Dept. of Computer Science & Engineering, MPGI School of Engineering, Nanded, Maharashtra, India*
[2]*HOD, Dept. of Computer Science & Engineering, MPGI School of Engineering, Nanded, Maharashtra, India*
[3]*Assistant Prof., Dept. of Computer Science & Engineering, MPGI School of Engineering, Nanded, Maharashtra, India*

Abstract - *Cloud computing enables the users to remotely store their data in a server and provide services on-demand. Cloud storage is the best way to handle our information securely. Data security and privacy are the critical issues. There are many encryption technologies used to share data securely. One of the best ways is CP-ABE is to solve challenging problem of secure data sharing scheme in cloud computing. Only authorized users are able to encrypt and decrypt data. Each user has the set of attributes. The layered access structure are integrated into single access structure .The hierarchical files are encrypted with integrated access structure. Ciphertext time cost of encryption is saved. Final Implementation gives that linearly increasing the encryption and decryption time as number of attributes are increased. In this paper an efficient file hierarchy attribute based encryption scheme is proposed.*

Key Words*: *Cloud Computing, data sharing, file hierarchy ciphertext-policy, attribute based encryption

1. INTRODUCTION

Cloud Computing can be described as web service oriented computing that provides an environment which acts as a service in delivering software and information management in a way that would have typically only been available in product format. This is done through personal devices – such as a laptop – that would access the services available through the network of servers that is called the "cloud".

1.1 Overview

Cloud Computing is the use of hardware and software to deliver a service over a network (typically the Internet). ... An example of a Cloud Computing provider is Google's Gmail. Gmail users can access files and applications hosted by Google via the internet from any device. Cloud Computing is to protect data from leaking, users need to encrypt their data before shared.

Cloud computing poses privacy concerns because the service provider can access the data that is in the cloud at any time. It could accidentally or deliberately alter or even delete information. Many cloud providers can share information with third parties if necessary for purposes of law and order even without a warrant. That is permitted in their privacy policies, which users must agree to before they start using cloud services. Solutions to privacy include policy and legislation as well as end users' choices for how data is stored. Users can encrypt data that is processed or stored within the cloud to prevent unauthorized access[1] .

Role based authentication is a combination of symmetric key cryptography and public key cryptography where by every encryption process needs data, public key, group key, policy. a policy is a set of rule that can be specified as chain also for e.g., in the context of hospital a policy can be given as {doctor, patient} which means anybody from the doctors group or patient group can simultaneously decrypt the document on the other hand a policy can be specified as chain policy for instance{doctor},{patient} this is known as nested policy .In such cases a patient can decrypt the document only when that is decrypted by doctors first, Policy based encryption is becoming popular in an enterprise context where different authorities require different permission and privacy settings for the access of the records. In this work we want to develop a novel CP-ABE[2] based search technique in an enterprise hospital context deployed in a local cloud with fog computing architecture ,our proposed system will offer different level of encryption, decryption, authentication, authorization and privacy setting for doctors, administrators and patients .we also propose to use a machine learning base system to diagnose abnormality in the medical image. In this work we demonstrate the use of CP-ABE with human entities as well as i n the context of machine learning the overall work demonstrate the entire process of medical scanning in an enterprise hospital application both plain record encryption and image encryption with the help of CP-ABE.

Problem definition:

CP-ABE is derived from AES and it is extremely complicated mathematically, CP-ABE encryption not only encrypts the data with a key but at the same time embeds the access policy, because access policy can be changed, the overall decryption process is also extremely complicated, therefore one of the major issue.

Issues:

1. Access Policy Management:

Implementing CP-ABE based system is, the design issue of appropriate forming the group, generating the group keys and managing the access policies.

2. Attack Prevention:

As CP-ABE scheme to decrypt the key, one of major issues with the system is that anybody acquiring a group key, a drawback can overcome by incorporating the private key also in the decryption process not only decryption authority require the group key but at the same time it on private key.

3. As our proposed work implement CP-ABE based encryption both record as well as with the images, the decryption and encryption of such a system using on hybrid records become a huge issue.

4. Bandwidth and latency Management:

As medical data is sensitive and requires a faster processing and because CP-ABE based encryption adds huge processing overhead ,a huge issue in such system is to develop systems with optimal processing and communication latency.

Challenges:

1. The major challenge with CP-ABE based encryption is creating mathematical model of encryption on the top of AES encryption schema that supports changed privacy. Simple form of CP-ABE encryption allows the user to specify the access policies as the simple set{doctor ,patient},however more complicated CP-ABE architecture allows the user to embed a complex set of policies where by policy itself can be nested designing and implementation of such a system and maintaining the integrity of the policy chain is extremely difficult.

2. Handling Media Data:

As most of the hospital or enterprise application not only deals with text data ,but also other forms of data like images, developing an algorithm that holds good for both text as well as image(binary record) is of extremely challenging serve.

3.Data Size:

Because CP-ABE is developed on the top of AES which is block encryption technique, it accepts the data to multiplier of block size. However in most cases the record will not be multiplier of the block size, padding of the data at the time of encryption and removal of padding is the challenging task.

2. LITERATURE SURVEY

The literature survey that containing study of different schemes available in Attribute Based encryption(ABE). An efficient file hierarchy attribute-based encryption scheme (FH-CP-ABE) is proposed by Shulan Wang, JunweiZhou, Joseph K. Liu, Jianping Yu, Jianyong Chen and WeixinXie. The layered access structures are integrated into a single access structure, and then the hierarchical files are encrypted with the integrated access structure. The cipher text components related to attributes could be shared by the files. Therefore, both cipher text storage and time costs of encryption are saved. Moreover, the proposed scheme is proved to be secure under the standard assumption. In this study, an efficient encryption scheme based on layered model of the access structure is proposed in cloud computing, which is named file hierarchy CP-ABE scheme (or FH-CP-ABE, for short). FH-CP-ABE extends typical CPABE with a hierarchical structure of access policy, so as to achieve simple, flexible and fine-grained access control.

2.1 Attribute Based Encryption

An attribute based encryption scheme introduced by Sahai and Waters in 2005 and the goal is to provide security and access control. Attribute-based encryption (ABE) is a public-key based one to many encryption that allows users to encrypt and decrypt data based on user attributes. In which the secret key of a user and the cipher text are dependent upon attributes (e.g. the country she lives, or the kind of subscription she has). In such a system, the decryption of a cipher text is possible only if the set of attributes of the user key matches the attributes of the cipher text. Decryption is only possible when the number of matching is at least a threshold value d. Collusion-resistance is crucial security feature of Attribute-Based Encryption [3]-[5]. An adversary that holds multiple keys should only be able to access data if at least one individual key grants access. The problem with attribute based encryption (ABE) scheme is that data owner needs to use every authorized user's public key to encrypt data. The application of this scheme is restricted in the real environment because it uses the access of monotonic attributes to control user's access in the system.

2.2 Key Policy Attribute Based Encryption

It is the modified form of classical model of ABE. Users are assigned with an access tree structure over the data attributes. Threshold gates are the nodes of the access tree. The attributes are associated by leaf nodes. To reflect the access tree Structure the secret key of the user is defined. Cipher texts are labeled with sets of attributes and private keys are associated with monotonic access structures that control which cipher texts a user is able to decrypt. Key Policy Attribute Based Encryption (KP-ABE) scheme[6] is designed for one-to-many communications.

KP-ABE scheme consists of the following four algorithms:

Setup : Algorithm takes input K as a security parameter and returns PK as public key and a system master secret key MK.PK is used by message senders for encryption. MK is used to generate user secret keys and is known only to the authority.

Encryption : Algorithm takes a message M, the public key PK, and a set of attributes as input. It outputs the ciphertext E.

Key Generation: Algorithm takes as input an access structure T and the master secret key MK. It outputs a secret key SK that enables the user to decrypt a message encrypted under a set of attributes if and only if matches T.

Decryption : It takes as input the user's secret key SK for access structure T and the ciphertext E, which was encrypted under the attribute set . This algorithm outputs the message M if and only if the attribute set satisfies the user's access structure T.

Limitations of KP-ABE:-

1. Encryptor cannot decide who can decrypt the encrypted data. It can only choose descriptive attributes for the data, and has no choice but to trust the key issuer. KPABE is not naturally suitable to certain applications. For example, sophisticated broadcast encryption where users are described by various attributes and in this, the one whose attributes match a policy associated with a ciphertext, it can decrypt the ciphertext. KP-ABE scheme supports user secret key accountability. It is providing fine grained access but has no longer with flexibility and scalability.

2. Expressive Key Policy Attribute Based Encryption**:-** In KP-ABE, enables senders to encrypt messages with a set of attributes and private keys are associated with access tree structure. Access tree structure specifies which all the ciphertexts the key holder is allowed to decrypt. Expressive key-policy attribute-based encryption (KPABE) schemes allow for non-monotonic access structures. Non monotonic access tree structures are those may contain negated attributes and with constant cipher-text size. This is more efficient than KP-ABE.

2.3 Ciphertext policy attribute based encryption

It introduced the concept of another modified form of ABE called CP-ABE that is Ciphertext Policy Attribute Based Encryption. In CP-ABE scheme, attribute policies are associated with data and attributes are associated with keys and only those keys that the associated attributes satisfy the policy associated with the data are able to decrypt the data. CP-ABE works in the reverse way of KP-ABE. In CP-ABE the ciphertext is associated with an access tree structure and each user secret key is embedded with a set of attributes. In ABE, including KP-ABE and CP-ABE, the authority runs the algorithm Setup and Key Generation to generate system MK, PK, and user secret keys. Only authorized users (i.e., users with intended access structures) are able to decrypt by calling the algorithm Decryption. In CP-ABE, each user is associated with a set of attributes. His secret key is generated based on his attributes. While encrypting a message, the encryptor specifies the threshold access structure for his interested attributes. This message is then encrypted based on this access structure such that only those whose attributes satisfy the access structure can decrypt it. With CP ABE technique, encrypted data can be kept confidential and secure against collusion attacks.

CP-ABE scheme consists of following four algorithms:

1. Setup : This algorithm takes as input a security parameter κ and returns the public key PK as well as a system master secret key MK. PK is used by message senders for encryption. MK is used to generate user secret keys and is known only to the authority.

2.Encrypt : This algorithm takes as input the public parameter PK, a message M, and an access structure T. It outputs the ciphertext CT.

3.Key-Gen : This algorithm takes as input a set of attributes associated with the user and the master secret key MK. It outputs a secret key SK that enables the user to decrypt a message encrypted under an access tree structure T if and only if matches T.

4.Decrypt : This algorithm takes as input the ciphertext CT and a secret key SK for an attributes set . It returns the message M if and only if satisfies the access structure associated with the ciphertext CT. In CP-ABE depends how attributes and policy are associated with cipher texts and users‟ decryption keys. In a CP-ABE scheme, a ciphertext is associated with a monotonic tree access structure and a user's decryption key is associated with set of attributes. In this scheme, the roles of ciphertexts and decryption keys are switched as that in KP-ABE.

Limitations of CP-ABE:-

However, basic CP-ABE schemes are still not fulfilling the enterprise requirements of access control which require considerable flexibility and efficiency. CP-ABE has limitations in specifying policies and managing user attributes. In a CP-ABE scheme, decryption keys only support user attributes that are organized logically as a single set, so users can only use all possible combinations of attributes in a single set issued in their keys to satisfy policies. For realizing complex access control on encrypted data and maintaining confidential-ability, CP-ABE can be used. Encrypted data can be kept confidential even if the storage server is un-trusted; moreover, our methods are secure against collusion attacks[7]. KP-ABE uses attributes to describe the encrypted data and built policies into user's keys. In other hand CP-ABE, attributes are used to describe a user's credentials. Data encryptor determines a policy for who can decrypt.

3. DESIGN GOALS

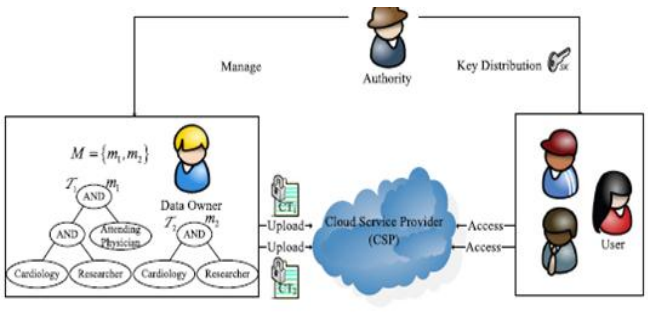

Fig. 1. An example of secure data sharing in cloud computing.

Authority-accepts the user enrollment and creates some parameters.

Cloud service provider (CSP) -is the manager of cloud servers and provides multiple services for client.

Data owner -encrypts and uploads the generated cipher text to CSP. It has large data needed to be stored and shared in cloud system.

User -downloads and decrypts the interested cipher text from CSP.

The shared files usually have hierarchical structure. That is, a group of files are divided into a number of hierarchy subgroups located at different access levels. If the files in the same hierarchical structure could be encrypted by an integrated access structure, the storage cost of cipher text and time cost of encryption could be saved.

3.1 Existing Scheme

CP-ABE system in the past has been used in the context of text records where text records are given various label of privacy and keys to different groups .CP-ABE byte design does not support media and binary records .Due to this disadvantage it cannot be used in many of the practical enterprise application and generally is limited to various text based searching and indexing technique.

3.2 Proposed Scheme

In order to overcome this basic drawback of CP-ABE based systems we propose a novel updated CP-ABE system which can be used for both text as well as binary(image records) we develop medical application where patient can register once the patient is registered their text record will be encrypted with privacy setting of admins and doctors patient personal record such as phone number and email-id will be encrypted with an access to only patient and admin as such a doctor would be able to view the patient and his case history but not the personal information ,the admin can upload the medical image(brain tumor) with privacy settings of only doctors and patients. A doctor upon viewing the medical image through a machine learning system. The result of machine learning system is a set of feature vector which will again be encrypted with the policy of only machine learning. The doctor will be able to see whether a particular record is abnormal or normal that information is again encrypted with the policy of doctor and that particular patient therefore a patient can view his own record, medical diagnosis observation a doctor will be able to see the patient general information, case history and the medical images and diagnosis but a doctor will not able to visualize the images of the doctors of the other patients a doctor will not able to visualize the personal information of the patient, the admin on the other hand would be able to see all the information of the patient along with their personal information but will not able to view medical diagnosis reports.

3.3 Computation Cost on Data Owner

The layered model of access structure is provided so as to achieve multiple hierarchical files sharing. The files are encrypted with one integrated access structure. So, data owner can encrypt the different levels of the files and generate an integrated ciphertext only executing the encryption algorithm one time. Especially, some common attributes should be computed only once instead of many times since each common attribute is appeared in the integrated access structure one time, where the common attribute denotes that it is appeared in multiple access sub-trees associated with k hierarchical files. Assume that there are n common attributes appeared in the m($m \leq k$) access sub-trees associated with the k hierarchical files, the computation workload of the common attributes about ciphertext C(x,y) and C'(x,y) is reduced by $2n(m-1/m)$, thus the encryption efficiency of data owner is also improved.

3.4 Computation Cost on User

In decryption process, users can decrypt all of his authorization files with computation of secret key once since transport nodes are added in the access structure with k level nodes. And the bilinear pairing operation of each common nodes used in multiple access sub-trees of the files is computed only once since each common node is also appeared in the integrated access structure one time. Assume that there are n common nodes appeared in the m($m \leq k$) access sub-trees associated with the k hierarchical files, the bilinear pairing computation cost of the common nodes about decryption Decrypt Node(CT, SK,(x, y)) is also reduced by $2n(m-1/m)$ if the user needs to decrypt the k files.

4. CONCLUSION AND FUTURE WORK

In this paper, the proposed scheme gives the encryption and decryption time which is linearly increasing as the number of attributes are increasing. Therefore, both cipher text storage and time cost of encryption are saved. The proposed scheme has an advantage that users can decrypt all authorization files by computing secret key once. Thus, the time cost of decryption is also saved if the user needs to decrypt multiple files. CP-ABE an adjustment of Attribute Based Encryption (ABE) for the reasons for giving certifications towards the provenance the delicate information Our scheme also enables dynamic modification of access policies o supports efficient on-demand user/attribute revocation and break-glass access under emergency scenarios. From the survey we understand that some amount of work has been done in the field of cloud computing for several security issues. It can be applied to achieve scalable, flexible, security, privacy, data confidentiality and fine-grained access control of outsourced data in cloud computing. There is more scope for future research in the field of secure data sharing in the cloud. We proposed a scheme for efficient identity-based user

revocation in multi-authority CP-ABE. In the future, our work can be continued in several directions. Securely forwarding the revocation related computations to the CSP (or even to the user). The security of our construction is proved in the generic bilinear group model, although we believe it would be possible to achieve full security by adapting the dual system encryption methodology. This type of work would be interesting even if it resulted in a moderate loss of efficiency from our existing system.

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] Y. Yang, J. K. Liu, K. Liang, K.-K. R. Choo, and J. Zhou, "Extended proxy-assisted approach: Achieving revocable fine-grained encryption of cloud data," in Proc. 20th Eur. Symp. Res. Comput. Secur. (ESORICS), vol. 9327. Sep. 2015, pp. 146–166.

[3] Sphurti Atram, N. R. Borkar A Review Paper on Attribute-Based Encryption Scheme in Cloud Computing 2017

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

[5] 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.

[6] V. Goyal, O. Pandey, A. Sahai, and B.Waters"Attribute-based encryption for fine-grained access control of encrypted data," in Proceedings of the 13th ACM conference on Computer and communications security, pp. 89{98, 2006}

[7] Minu George1, Dr. C.Suresh Gnanadhas2, Saranya.K3 , A Survey on Attribute Based Encryption Scheme in Cloud Computing.2013