A Hierarchical Attribute-Based EncryptionFor Mobile Cloud Data Security

Swathi Dodla & Sumathi Eedur
[1]PG Scholar, Dept of CSE, Andhra Engineering College, Atmakur, AP, India.
2Assistant Professor, Dept of CSE, Andhra Engineering College, Atmakur, AP, India.

Abstract: *Cloud computing, as a promising computing model, enables users to remotely storetheir data into a cloud so as to enjoy scalable services on-demand. 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 entrusted CSPs, a usual 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, and scalability, 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 cipher text-policy Attribute-Based Encryption (CP-ABE) system.*

Keywords

Cloud computing, hierarchical attribute-based encryption, fine-grained access control, scalability

I.INTRODUCTION

Cloud computing is rising computing technology that uses Internet. It consists of the use of computing resources that are delivered as a service over a network. In cloud computing model users have to give access to their data for storing and performing the desired business operations. Hence cloud service provider must provide the trust and security, as there is valuable and sensitive data in huge amount stored

on the clouds. There are concerns about flexible, scalable and fine grained access control in the cloud

Computing. For this purpose, there have been many of the schemes, proposed for encryption. Such as simple encryption technique that is classically studied. We are going to discuss about the Attribute-Based Encryption (ABE) schemes and how it has been developed and modified further into Key Policy. Attribute based encryption (KP-ABE). Cipher-text Policy Attribute Based Encryption (CP-ABE) and further it has been proposed as CP-ASBE and furthermore HABE and HASBE so on. This is according to how flexible, scalable and fine grained access control is provided by each scheme. Cloud computing has rapidly become a widely adopted paradigm for delivering services over the internet. Therefore cloud service provider must provide the trust and security, as there is valuable and sensitive data in large amount stored on the clouds. For protecting the confidentiality of the stored data, the data must be encrypted before uploading to the cloud by using some cryptographic algorithms. In this paper we going to discuss about attribute based encryption scheme and its categories. With the burgeoning of network technology and mobile terminal, Meanwhile, cloud computing is one of the most promising application platforms to solve the explosive expanding of data sharing. In cloud computing, to protect data from leaking, users need to encrypt their data before being shared. Access control is paramount as it is the first line of defense that prevents unauthorized access to the share data. Recently, attribute-based encryption (ABE) has been attracted much more attentions since it can keep data privacy and realize fine-grained, one-to-many, and non interactive access control. Cipher text -policy attribute based encryption (CP-ABE) is one of feasible schemes which has much more flexibility and is more suitable for general applications 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. 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 ciphertext and time cost of encryption could be saved. A patient divides his PHR information *M* into two parts: personal information *m*1 that may contain the patient"s name, social security number, telephone number, home address, etc. The medical record *m*2 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 information *m*1 and *m*2 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 researcher, and the converse is not necessarily true. 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. 3 below) 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.

II.

LITERATURE SURVEY

A. Attribute based encryption (ABE):- First introduced the attribute based encryption (ABE) for enforced access control throughpublic key cryptography. The main goal for these models is to provide security and access control. The main aspects are toprovide flexibility, scalability and fine grained access control. In classical model, this can be achieved only when user and server arein a trusted domain. But what if their domains are not trusted or not same? So, the new access control scheme that is „AttributeBased Encryption (ABE)" scheme was introduced which consist of key policy attribute based encryption (KP-ABE). As compared

with classical model, KP-ABE provided fine grained access control. However it fails with respect to flexibility and scalability when

authorities at multiple levels are considered. In ABE scheme both the user secret key and the ciphertext are associated with a set ofattributes. A user is able to decrypt the cipher-text if and only if at least a threshold number of attributes overlap between the cipher-text and user secret key. Different from traditional public key cryptography such as Identity-Based Encryption [3], ABE is

implemented for one-to many encryption in which cipher-texts are not necessarily encrypted to one particular user, it may be for more than one number of users. In Sahai and Waters ABE scheme, the threshold semantics are not very expressive to be used for

designing more general access control system. Attribute-Based Encryption (ABE) in which policies are specified and enforced in

the encryption algorithm itself. The existing ABE schemes are of two types. They are Key-Policy ABE (KP-ABE) scheme and

Cipher text-Policy ABE (CPABE) scheme. That can be discussed further.

B. Key Policy Attribute Based Encryption (KP-ABE):- It is the modified form of classical model of ABE. Exploring KP-ABEscheme, attribute policies are associated with keys and data is associated with attributes. The keys only associated with the policy that is to be satisfied by the attributes that are associating the data can decrypt the data. Key Policy Attribute Based Encryption (KP-ABE) scheme is a public key encryption technique that is designed for one-to-many communications. In this scheme, data is associated with the attributes for which a public key is defined for each. Encrypter, that is who encrypts the data, is associated with the set of attributes to the data or message by encrypting it with a public key. Users are assigned with an access tree structure over the data attributes. The nodes of the access tree are the threshold gates. The leaf nodes are associated with attributes. The secret key of the user is defined to reflect the access tree structure. Hence, the user is able to decrypt the message that is a ciphertext if and only if the data attributes satisfy the access tree structure. In KP-ABE, a set of attributes is associated with ciphertext and the user"s decryption key is associated with a monotonic *access tree structure.* When the attributes associated with the ciphertext satisfy the access tree structure, then the user can decrypt the ciphertext. In the cloud computing, for efficient revocation, an access control mechanism based on KP-ABE and a reencryption technique used together. It enables a data owner to reduce most of the computational overhead to the servers. The KP-ABE scheme provides fine-grained access control. Each file or message is encrypted with a symmetric data encryption key (DEK), which is again encrypted by a public key, that is corresponding to a set of attributes in KP-ABE, which is generated corresponding to an access tree structure. The encrypted data file is stored with the corresponding attributes and the encrypted

DEK. If and only if the corresponding attributes of a file or message stored in the cloud satisfy the access structure of a user"s key, then the user is able to decrypt the encrypted DEK. That can be used to decrypt the file or message. KP-ABE scheme consists of the following four algorithms:

1. Setup: This algorithm takes as input a security parameterκ and returns the public key PKand 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. Encryption: This algorithm takes a message M, the public key PK, and a set of attributes as input. It outputs the cipher text E.

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

4. Decryption: It takes as input the user"s secret key SK foraccess structure T and the cipher text 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 cipher text, it can decrypt the cipher text. 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 attributesand 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.

C. Cipher Text 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 cipher text 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 parameterκ and returns the public keyPK as well as a system master secret keyMK. 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 asecret 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 cipher text CT and a secret key SK for an attributes set . It returns the message M ifand only if satisfies the access structure associated with the cipher text CT. In CP-ABE depends how attributes and policy are associated with cipher texts and users‟ decryption keys. In a CP-ABE scheme, a cipher text 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 cipher texts 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. 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‟scredentials. Data encryptor determines a policy for who can decrypt.

D. Ciphertext Policy Attribute-Set Based Encryption (CPASBE):-

As compared to CP-ABE scheme in which the 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. To solve this problem, ciphertext-policy attribute-set based encryption

(CP-ASBE or ASBE for short) is introduced by *Bobba, Waters et al* [7]. ASBE is an extended form of CPABE which organizes user attributes into a recursive set structure. Ciphertext Policy Attribute Set Based Encryption (CP-ASBE) is a modified form of CP-ABE. It differs from existing CP-ABE schemes that represent user attributes as a monolithic set in keys. It organizes user attributes into a recursive set based structure and allows users to impose dynamic constraints on how those attributes may be combined to satisfy a policy. The CP-ASBE consists of recursive set of attributes. The desirable feature and the recursive key structure is implemented by four algorithms, Setup, KeyGen,

Encrypt, and Decrypt

1. **Setup:** Here is the depth of key structure. Take as input adepth parameter „d". It outputs a public key PK andmaster secret keyMK.

2. Key-gen: Takes as input the master secret key*MK*, the identity of user*u*, and a key structure*A*. It outputs a secret key SK foruser u.

3. Encrypt: Takes as input the public key PK, a message M, and an access tree T . It outputs a ciphertext CT.

4. Decrypt: Take as input a ciphertext CT and a secret key SK for user u. It outputs a message m . If the key structure A associatedwith the secret key SK, satisfies the access tree T, associated with the ciphertext CT, then m is the original correct message M. Otherwise, m is null. Specifically CP-ASBE allows- User attributes are organized into a recursive family of sets and Allowing attributes to combine from multiple sets. Thus, by grouping user attributes into sets and no restriction on how they can be combined, CP-ASBE can support compound attributes. More flexibility and fine grained access is provided by AP-ASBE. Similarly, multiple numerical assignments for a given attribute can be supported by placing each assignment in a separate set as well as placing it into a single set.

Limitations:-

The challenge in constructing a CP-ASBE scheme is in selectively allowing users to combine attributes from multiple sets within a given key. There is challenge for preventing users from combining attributes from multiple keys.

III. CONCLUSION

This paper made a survey on the Improving the Security on Public Health Record System in Cloud Computing. And also made a detailed study about what are the techniques is needed for security the Health Record System. Attribute Based Encryption is the good technique to securing the Health records. It is efficient in the Conjunctive Property. But somewhat limitations on MA-ABE in real time with the property of Disjunctive as well as it had the little bit problem while revocation. Because it can be affect the non-revoked users. So move to the Attribute Based Broadcast Encryption. It satisfies the Disjunctive Property also and handles the revocation perfectly. Identity Based Encryption is the better way to provide the authentication for the Public Health Record System. homomorphic encryption with data auditing is used to verify the trustworthiness of third party auditor.

REFERENCES

[1] Sahai and B. Waters. "Fuzzy Identity Based Encryption.", In Advances in Cryptology – Eurocrypt, volume 3494 of LNCS, pages 457–473. Springer, 2005.

[2] Li, M., Lou,W., Ren, K., " Data security and privacy in wireless body area networks", IEEE Wireless Communications Magazine (February 2010).

[3] M. Li, S. Yu, K. Ren, and W. Lou, "Securing Personal Health Records in Cloud Computing: Patient -Centric and Fine-Grained Data Access Control in Multi-Owner Settings", Proc. Sixth Int‟l ICST Conf. Security and Privacy in Comm. Networks (SecureComm ‟10),pp. 89 -106, Sept. 2010. Prof.Y.B.Gurav et al, International Journal of Computer Science and Mobile Computing, Vol.3 Issue.2, February- 2014, pg. 617-625 © 2014, IJCSMC All Rights Reserved 625

[4] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data,"Proc. 13th ACM Conf. Computer and Comm. Security (CCS ‟06),pp. 89-98, 2006.

[5] Ming LiShucheng Yu, Yao Zheng,KuiRen, and Wenjing Lou, "Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption", IEEE transactions on parallel and distributed systems, vol. 24, no. 1, january 2013.

[6] L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker, "Ciphertext-Policy Attribute-Based Threshold Decryption with Flexible Delegation and Revocation of User Attributes", 2009.

[7] L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker, "Ciphertext-Policy Attribute-Based Threshold Decryption with Flexible Delegation and Revocation of User Attributes", 2009.
NelloreDt-524322(A.P).

[8] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute Based Data Sharing with Attribute Revocation," Proc. Fifth ACM Symp. Information, Computer and Comm. Security (ASIACCS ‟10), 2010.

[9] S. Narayan, M. Gagne´, and R. Safavi-Naini, "Privacy Preserving EHR System Using Attribute-Based Infrastructure", Proc. ACM Cloud Computing Security Workshop (CCSW ‟10), pp. 47-52, 2010.

[10] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-Policy Attribute-Based Encryption", Proc. IEEE Symp. Security and Privacy (SP ‟07), pp. 321-334, 2007.

[11] Q.Wang et al.,"Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing," Proc. ESORICS „09, Sept. 2009, pp. 355–70.

Author's Profile:

SWATHI DODLA has received her B.Tech Degree in Computer Science Engineering from Sri Raghavendra institute of science and technology, affiliated to JNTU, Ananthapur in 2016 and Pursuing M.Tech degree in Computer Science & Engineering in Andhra Engineering College, Atmakur, affiliated to JNTUA, Anantapur in 2019.

SUMATHI EEDUR has
l her M.Tech
gree from ANU a
ech (CSIT) from JNTU. Currently working as an Assistant Professor in Andhra Engineering College, Atmakur,