Data Security in Cloud Using Attribute Based Encryption with Efficient Keyword Search

Ms.Dipali Patil, Dr.P.K.Deshmukh

Abstract— In today's world there are many new challenges for security of data and access control when users outsource sensitive data for sharing on third party server known as cloud servers, which are not within the same trusted domain as data owners. The existing technique used to maintain confidentiality of personal medical record (PMR) against untrusted servers by disclosing data decryption keys only to authorized users. However, in doing so, these solutions inevitably introduce complexity in key management also burden on the data owner in data management well as in key management. The problem of simultaneously achieving security and data confidentiality and fine-grainedness of access control still remains unresolved. This paper addresses this challenge 1) Key management, 2) Defining and enforcing access policies based on data attributes, and, 3) Keyword search over the encrypted data. PMR(patient medical record)system users need to deal with complicated key management problem to accomplish fine-grained access control when their PMRs are encrypted using symmetric key cryptography or asymmetric key cryptography .With our scheme multi-authority attribute based access control (MA-ABAC) we can reduce the key management complexity for owners and users. For this users are divided into the two domains; professional domain and personal domain. To achieve security of PMR, key management, user revocation and efficient keyword search exploiting KP-ABE, Multi-authority attribute based access control(MA-ABAC), and uniquely combining it with techniques of proxy re-encryption.

Index Terms— Attribute based encryption, Cloud computing, Fine-grained access control, KP-ABE, MA-ABAC, User Revocation, Proxy Re-encryption.

1 INTRODUCTION

The cloud itself may be a set of hardware, networks, storage, services and interfaces that change the delivery of computing as a service. Cloud services embrace the delivery of package, infrastructure and storage over the net (either as separate parts or an entire platform) supported user demand. Because of that information security becomes important considerations from users after they store sensitive data on cloud servers. These considerations originate from actual fact that cloud servers are sometimes operated by business suppliers that are very doubtless to be outside of the trustworthy domain of the users. Information confidential against cloud servers is thus often desired once users source information for storage within the cloud. There are cases during which cloud users themselves are content suppliers. They publish information on cloud servers for sharing and want fine-grained information access management in terms of that user (data consumer) has the access privilege to that forms of information. To stay sensitive user information confidential against untrusted servers, existing solutions sometimes apply cryptanalytic strategies by revealing information decoding keys solely to approved users. However, in doing thus, these solutions inevitably introduce a significant computation overhead on the information owner for key distribution and information management once fine grained data access management is desired, and therefore don't scale well[9]. The matter of at the same time is achieving fine-grained quantifiability and information confidentiality of access management still remains unresolved. This paper addresses the scheme which is based on the set of attributes. The access structure of each user can thus define as a unique logical expression over these attributes to reflect the scope of data files that the user is allowed to access. For this we define the public key components as per their attributes. In this data files are encrypted using public key. The user is able to decrypt the data file by using the secret key if the data file attributes satisfies his/her access structure. Here the complexity of encryption is interrelated to the number of attributes associated to the file and is not dependent on the number of users in the system. The multiple owners can encrypt their data with different set of keys. The user who wants PMR, they required to obtain key from the owner because patients are not always online. On one hand maintain central authority that is responsible for key management. But disadvantage is that central authority is semi-trusted. PMR may be stored on different locations, such as an Internet database, a provider's PMR, the owner's personal computer. Patients can access their own data, but always they do not see for anyone else may access it. In this paper we divide the system users into two domains first is personal domain and another one is professional domain. In a personal domain there are only limited users such as friend, family relation and in professional domain more no of users such as healthcare, researchers, students etc. Because of more no. of users in public domain, security problem arises as well as key management is very complex task. To solve this problem we use multi-authority attrib-

- *Ms.Dipali L. Patil is currently pursuing masters degree program in Computer engineering in Savitribai Phule Pune University,India. E-mail: patildipali88@gmail.com*
- *Dr.Pradeep K . Deshmukh is currently working as professor in computer engineering department RSCOE Tathwade ,Savitribai Phule Pune University, India. E-mail:pkdeshmukh9@gmail.com*

International Journal of Scientific & Engineering Research Volume 7, Issue 1, January-2016
ISSN 2229-5518

ute based access control mechanism (MA-ABAC). Because of this there requires more no. of attribute authority in public domain; achieved with the help of MA-ABAC [3]. User revocation is also important when user leave the system. User sends a keyword as input to the system and will get the output as file which contains respective keyword only when they satisfy the access policy set by the owner (patient).

2 Related Work

[1] Li, Yu, Zheng proposed a framework which enhance an existing MA-ABE scheme to handle efficient and on-demand user revocation, and prove its security.[2] Wenhai Sun*,Hui proposed first attribute-based keyword search technique with user revocation (ABKS-UR) that enables fine-grained (i.e. file-level) search authorization.[3]Ren, and W. Lou proposed a novel framework for access control to PHRs within cloud computing environment. To enable fine-grained and scalable access control for PHRs;they used attribute based encryption (ABE) techniques to encrypt each patients' PHR data.[4] Goyal, Pandey, Sahai, developed a new cryptosystem for fine-grained sharing of encrypted data that they call Key-Policy Attribute-Based Encryption (KP-ABE). [5]Lewko, Okamoto proposed a new approach on bilinear pairings using the notion of dual pairing vector spaces and also present a fully secure hierarchical PE scheme under the assumption whose size does not depend on the number of queries.[6]Yu, N. Cao proposed two novel solutions for APKS based on a hierarchical predicate encryption (HPE), one with enhanced efficiency and the other with enhanced query privacy.[7] W. Sun, B. Wang, Hou proposed a tree-based index structure and various adaption methods for multi-dimensional (MD) algorithm to improve the search efficiency.[8] J. Camenisch and A. Lysyanskaya proposed a technique to prevent misuse of anonymity, scheme is the first to offer optional anonymity revocation for particular transactions and second offers separability means all organizations can choose their cryptographic keys independently of each other.[9] J. Hur and D.K. Noh proposed an access control mechanism using ciphertext-policy attribute-based encryption to enforce access control policies with efficient attribute and user revocation capability.[10]Yu,Wang ,Lou proposed technique of defining and enforcing access policies on data attributes, and allowing the data owner to delegate most of the working involved in fine grained data access control to untrusted cloud servers without releasing the data contents.[12] IBE scheme improves key-update efficiency on the side of the trusted party, while staying efficient for the users.This scheme based on the Fuzzy IBE primitive and binary tree data structure.[14] A new ABE scheme called Attribute-Based Encryption with Attribute Lattice (ABE-AL) which provides an methodology to implement comparison operations between attribute values on a poset derived from attribute lattice.[15]Authorized users have their own keys for performing operations on file. The scheme supports keyword search which enables the server to return only the encrypted data that satisfies an encrypted query without decrypting it. [17] Yang Yang focuses on the multiple sender and multiple user application scenario to provide a flexible search authorization searchable encryption (SE) scheme. The attribute based encryption (ABE) technology is used to support fine-grained access control and the synonym keyword search is enabled. [18] Zhou, Varadharajan presented a secure RBE-based hybrid cloud storage architecture that lets an organization to store data securely in a public cloud, while maintaining the sensitive information related to the organization's structure in a private cloud. [19] Described new techniques for remote searching on encrypted data using an untrusted server.

3 Preliminaries

3.1 Key Policy Attribute-Based Encryption(KP-ABE)

Data encryption is the most effective in regard to preventing sensitive data from unauthorized access. In earlier public key encryption or identity-based encryption systems, encrypted data is targeted for decryption by a single known user. To address these emerging needs, Sahai and Waters [4] introduced the concept of attribute-based encryption (ABE). As an alternative of encrypting to individual users, in ABE system, one can embed an access policy into the cipher- text or decryption key. Hence, data access is self-enforcing from the cryptography, needing no trusted mediator.

ABE can be viewed as an extension of the notion of identity-based encryption in which user identity is generalized to a set of expressive attributes instead of a single string specifying the user identity. Compared with identity-based encryption ABE has significant advantage that it achieves flexible one-to-many encryption as an substitute of one-to-one; it is envisioned as a promising tool for addressing the problem of secure and fine-grained data sharing and decentralized access control.

There are two types of ABE depending on which of private keys or cipher texts that access policies are associated with. KP-ABE is a public key cryptography primitive for one-to-many communications. In KP-ABE, files are associated with attributes for each of which a public key component is defined [5]. The encryptor associates the set of attributes to the message by encrypting it with the corresponding public key components. For each user an access structure is assigned, which is usually defined as an access tree over data attributes, i.e., inner nodes of the access tree are threshold gates and leaf nodes are associated with attributes. User secret key is defined to reflect the access structure so that the user is able to decrypt a cipher text if and only if the data attributes satisfy his access structure KP-ABE schemes are suitable for structured organizations with rules about who may read particular documents.
In a cipher text-policy attribute-based encryption (CP-ABE) system [9], when a sender encrypts a message, they specify a specific access policy in terms of access structure over attributes in the cipher text, stating what kind of receivers will be

International Journal of Scientific & Engineering Research Volume 7, Issue 1, January-2016
ISSN 2229-5518

able to decrypt the cipher text. Users possess sets of attributes and obtain corresponding secret attribute keys from the attribute authority. Such a user can decrypt a cipher- text if his/her attributes satisfy the access policy associated with the cipher text. Thus, CP-ABE mechanism is conceptually closer to earlier role-based access control method [18].

3.2 Proxy Re-encryption

A basic goal of public-key encryption is to allow only the key or keys selected at the time of encryption to decrypt the ciphertext or change the ciphertext to a different key needs re-encryption of the message with the new key, which gives access to the original clear text and to a reliable copy of the new encryption key.This seems a fundamental, and quite desirable, property of good cryptography; it should not be possible to change the key with which a message can be decrypted by an untrusted party. Here, on the other hand [1] Proxy Re-Encryption (PRE) is a cryptographic primitive in which a semi-trusted proxy is able to convert a cipher text encrypted under A's public key into another cipher text that can be opened by B's private key without seeing the underlying plaintext.A Proxy Re-Encryption scheme allows the proxy, given the proxy re-encryption key rkab, to translate cipher texts under public key pk a into cipher texts under public key pkb and vice versa [10].

3.2.1 Atomic Proxy cryptography

A basic goal of public-key encryption is to allow only the key or keys selected at the time of encryption to decrypt the cipher text. To change the cipher text to a different key requires re-encryption of the message with the new key, which implies access to the original clear text and to a reliable copy of the new encryption key.An atomic proxy function allows an untrusted party to convert cipher text between keys without access to either the original file or to the secret component of the old key or the new key.

3.3 User Revocation

In case of user revocation, the data owner define updated tree structure and data file re-encryption. Whenever the data owner revoke user, the data owner first determines a minimal set of attributes without which the leaving user's access structure will never be satisfied. Next, he updates tree structure.

3 System Architecture

In proposed system we divide the system users into the personal domain and professional domain. Personal domain users are like friends, family. Professional domain users are from different sectors healthcare, student, research etc. Owner encrypt PMR file and obtain secret key. Owner then again encrypt file by using different set of attributes with the particular access policy. For this we are using KP-ABE. While encrypting data in personal domain owner consider relation. If the user satisfies that relation then and then only he will able to access the file. In professional domain PMR file accessible to the user if he satisfies access policy given for the each attribute authority. Each attribute authority in system governs disjoint subset of user attributes. We are using MA-ABAC policies during encryption .Owner is free to set different policies. Owner can add/delete/modify the policy also they can dynamically change the policy. Our system also supports user revocation. User who wants file send a request as keyword to the cloud server they will get a file only when they satisfy the access policy set by the owner.

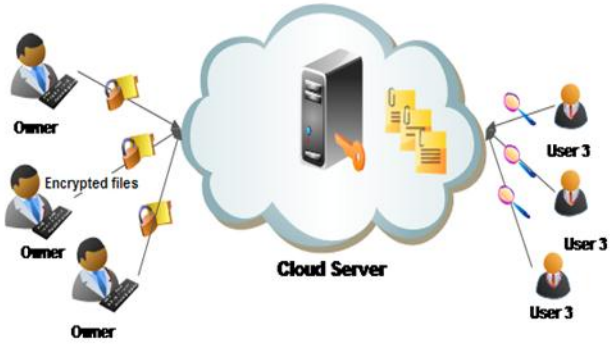

Fig.1. System Architecture for PMR Sharing

3 Methods

3.1 System Setup And Key Distribution

System defines universe of data attributes for personal domain users and professional domain users.Each PMR owner generates its public /master keys.public keys published via user's profile in an social-network(HSN).User from personal domain send s a request to get PMR file .Owner sends specific secret key when user satisfy the access policy set by the corresponding owner .when request is from professional domain they will get secret key from attribute authority

3.2 PMR Encryption

Owner outsource the encrypted PMR file to the cloud server. Each PMR file encrypted under the certain fine grained and attribute based access policy for users from professional domain and for the users from personal domain owner encrypt the file with attributes e.g relation .

3.3 Authorized Keyword Search And Access

Users from any domain search over the encrypted data. User send a request as a keyword to the cloud and will get file which contains that keyword ,only when user satisfy the access policy set by the owner.Only authorized users can decrypt the PMR file who have attribute based suitable key.

International Journal of Scientific & Engineering Research Volume 7, Issue 1, January-2016
ISSN 2229-5518

3.4 User Revocation

When user revoked the user will not get access to the file further.

3.4 Policy Updates

PMR owner can updates the access policy for existing PMR file.

3.6 Handle Dynamic Policy Change

Our scheme should support the dynamic add/modify/delete of part of the document access policies or data attributes by the owner.

4. Algorithms

4.1 AES

AES is symmetric key algorithm which uses single key for both encryption and decryption. AES is a block cipher with block length 128 bits. Encryption consists of 10 rounds. Except for the last round in each case, all other rounds are identical. Each round of processing includes one single-byte based substitution step, a row-wise permutation step, a column-wise mixing step, and the addition of the round key. The order in which these four steps are executed is different for encryption and decryption.

For encryption, each round consists of the following four steps:
1) Substitute bytes,
2) Shift rows,
3) Mix columns, and
4) Add round key.

For decryption, each round consists of the following four steps:
1) Inverse shift rows,
2) Inverse substitute bytes,
3) Add round key, and
4) Inverse mix columns.

4.2 KP-ABE Scheme with Efficient Keyword search, Proxy Re-encryption and User Revocation

The scheme composed of following algorithms which can be defined as follows:

- Setup
  Input: Security parameter i.e key size, Attribute universe
  Output: public key Pub, master key mk.
- Key Generation
  Input: Attribute set Ai, Attribute structure A.
  Output: Private key PRi of user ui.
- Encryption
  Input: PMR file, Pub, A
  Output: Encrypted file
- Search
  Input: Keyword k, files on storage F
  Output: Set of files fi contains respective keyword k
- Decryption
  Input: fi ,Ai, A,secret key Ski
  Output: Decrypted files that contains k .If attribute set Ai of user ui satisfies the attribute structure associated with file.
- User revocation
  Input: user id ,change tree structure
  Output: user revoked
- Proxy Re-encryption
  Input: user id, private key
  Output: Decrypted file

5. Evaluation

To evaluate the performance of AES design for encryption and decryption time of different size files such as 271 bytes, 464 bytes, 483 bytes, 487 bytes, 499bytes as follows.

TABLE 1
Time required for Encryption and Decryption of files with AES

AES			
SR.No.	File Size (bytes)	Encryption Time(ms)	Decryption Time(ms)
1	271	291	278
2	464	347	331
3	483	351	338
4	487	352	338
5	499	355	341

To evaluate keyword search time performance with lookup service, as the no. of files over the storage increases the time required to search the keyword over the file storage increases.

International Journal of Scientific & Engineering Research Volume 7, Issue 1, January-2016
ISSN 2229-5518

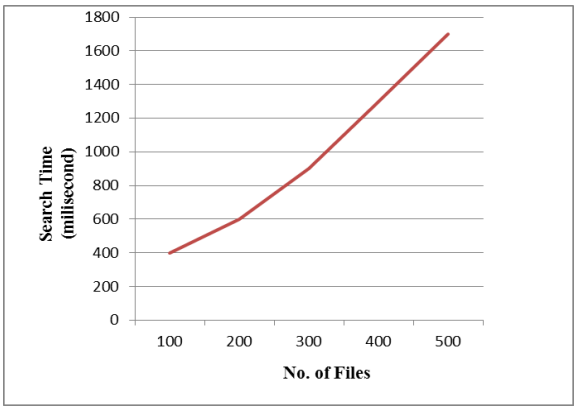

Fig.2 No.of files Vs Search Time

5. Conclusion And Fure Work

In this project we propose a scheme to achieve security in cloud by exploiting KP-ABE and uniquely combining it with techniques of MA-ABAC, proxy re-encryption, user revocation, keyword search. Moreover, our proposed scheme can reduce complexity of key management over the data owner and user by using MA-ABAC. Confidentiality of user access privileges achieved.Our scheme is safe under standard cryptographic models.In future we can use another method for keyword search and enhance the security.

Acknowledgment

I would like to thank my guide **Dr. Pradeep. K. Deshmukh** for giving me all the help and guidance I needed throught this project.

References

[1] M .Li, S.Yu, Yao Zheng, Kui Ren, Wenjing Lou ,"Salable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute Based Encryption",IEEE Trans. Parellel and Distributed Systems, Vol.24,No.1 Jan 2013.

[2] Wenhai Sun*,Hui Li*,Shucheng Yu,Thomas Hou,Wenjing Lou,"Protecting Your Right: Attribute-based Keyword Search with Fine-grained Owner-enforced Search Authorization in the Cloud",Proc.IEEE 978-1-4799-3360-0,2014

[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 Intl ICST Conf. Security and Privacy in Comm. Networks (SecureComm 10), pp. 89-106, Sept. 2010.

[4] V.Goyal, O. Pandey,A. Sahai, and B.Waters, "Attribute-based encryption for fine-grained access control of encrypted data", in Proc. ACM Conf.Computer and Communications Security, 2006, pp. 8998.

[5] Allison Lewko, Tatsuaki Okamoto, Amit Sahai, Katsuyuki Takashima, and Brent Waters,"Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption", In EUROCRYPT, pages 6291, 2010.

[6] M. Li, S. Yu, N. Cao, and W. Lou, "Authorized Private Keyword Search over Encrypted Personal Health Records in Cloud Computing", Proc. 31st Intl Conf. Distributed Computing Systems (ICDCS 11), June 2011.

[7]W. Sun, B. Wang, N. Cao, M. Li, W. Lou, Y. T. Hou, and H. Li, "Privacy preserving multi-keyword text search in the cloud supporting similarity based
ranking," in *Proc. of ASIACCS*. ACM, 2013, pp. 71–82.

[8] J. Camenisch and A. Lysyanskaya,"An efficient system for nontransferable anonymous credentials with optional anonymityrevocation", In: EUROCRYPT, 2001.

[9] J. Hur and D.K. Noh, "Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems", IEEE Trans. Parallel and Distributed Systems, vol. 22, no. 7, pp. 1214-1221, July 2011.

[10] S. Yu, C. Wang, K. Ren, and W. Lou," Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing", Proc. IEEE INFOCOM 10, 2010.

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

[12] A. Boldyreva, V. Goyal, and V. Kumar, "Identity-Based Encryption with Efficient Revocation", Proc. 15th ACM Conf. Computer and Comm. Security (CCS), pp. 417-426, 2008.

[13] Kan Yang,Xiaohua Jia," Expressive, Efficient, and Revocable Data Access Control for Multi-Authority Cloud Storage" IEEE Transactions on Parallel and Distributed Systems, Vol. 25, No. 7, July 2014 1735

[14]Y. Zhu, D. Ma, C. Hu, and D. Huang, "How to use attribute-based encryption to implement role-based access control in the cloud," in Proc. Int. Workshop Sec. Cloud Comput., 2013, pp. 33–40.

[15]C. Dong, G. Russello, and N. Dulay, "Shared and Searchable Encrypted Data for Untrusted Servers," J. Computer Security,vol. 19, pp. 367-397, 2010.

[16] Raghavendra S∗, Girish S∗, Geeta C M∗, Rajkumar Buyya†, Venugopal K R∗, S S Iyengar‡ and L M Patnaik," IGSK: Index Generation on Split Keyword for Search over Cloud Data", Intl conference on computing and network communications, 978-1-4673-7309-8/15/$31.00 ©2015 IEEE.

[17]Yang Yang[1,2],"Attribute-based data retrieval with semantic keyword search for e-health cloud",Proc. ACM Journal of Cloud Computing: Advances, Systems and Applications,DOI 10.1186/s13677-015-0034-8,2015

[18] Lan Zhou, Vijay Varadharajan and Michael Hitchens "Achieving

International Journal of Scientific & Engineering Research Volume 7, Issue 1, January-2016
ISSN 2229-5518

Secure Role-Based Access Control on Encrypted Data in Cloud Storage", IEEE Transactions on Information Forensics and Security, Vol. 8, No. 12, December 2013.

[19] D. X. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in *Proc. of S&P*. IEEE, 2000, pp. 44–55.