ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

Survey on Multi Authority ABE Scheme in Cross Domain Data Sharing

R.Shamini [#1], M.Revathi[#2]

Teaching fellow, Department of CSE, University College of Engineering (BIT Campus) , India[# 1&2]

ABSTRACT: Attribute Based Encryption (ABE) as the main primitives to protect the patient data stored on a semi-trusted. In ABE scheme, each patient can be identified by label which comprises the patient attributes. When Patient outsource the sensitive data for sharing on cloud system on cloud systems. Storing the patient records on untrusted storage makes secure data sharing a challenge issue. To keep sensitive user data confidential against untrusted cloud system. The existing system usually apply cryptographic methods by disclosing data decryption keys only to authorized user. The main challenges for cryptographic method include simultaneously achieving system scalability and fine grained data access control ,efficient key or user management ,data security, computational overhead and etc. To address these issues , in this paper we applied and enforcing access policies based on data attributes and enabling the data owner to delegate most computation intensive tasks to user revocation to untrusted server without disclosing data content to then. We achieve this goal by introducing multi authority attribute based encryption. Our proposed scheme also has salient features of user access privilege confidentiality ,dynamic modification of access policies or file attributes and user secret key accountability, supports efficient on-demand user or attribute revocation and break-glass access under emergency scenarios.

KEYWORDS: Cloud computing, Personal health records, data privacy, fine-grained access control, attribute based encryption, multiple authority ABE, user revocation, untrusted storage

I.INTRODUCTION

Cloud Computing, the long-held dream of computing as a utility, has the potential to change a large part of the IT industry, that making software even more attractive as a service and shaping the way IT hardware is designed and developed. Recent advances in IT have greatly facilitated remote data storage and sharing. New applications such as online social networks and online documents provide very convenient ways for people to store and share various data including personal profile, electronic documents and etc on remote online data servers. Cloud Computing, regarded as the future IT architecture, and even promises to provide unlimited and elastic storage resource (and other computing resources) as a service to cloud users in a very cost-effective way [3]. Although still at its previous stage, Cloud Computing has already drawn great attention, and its benefits have attracted an increasing number of users to outsource their local data centres' to remote cloud servers. Data security is a critical issue for remote data storage. On one hand, disclosure of confidential information, such as health records that stored on remote data servers has to be strictly protected before users have liberty to use the data services. Fine-grained data access control mechanisms often need to be in place to assure appropriate disclosure of sensitive data among multiple users. On the other hand, in remote data storage users do not physically possess their data. Remote data service providers are almost certain to be outside the users' trust domain, it not allowed to learn users' sensitive information stored on their servers. It turns out that users cannot rely on remote data servers to enforce access control policies like traditional access control [2] in which reference monitors should be fully trusted. User enforced data access control is thus highly desired for remote data storage. More generally, such an issue also exists in any untrusted storage, e.g., distributed data storage in Wireless Sensor Networks (WSNs), for which storage devices that are either owned by untrustworthy provider(s) or highly vulnerable to memory breach attacks, These concerns originate from the fact that cloud servers are usually operated by commercial providers which are very likely to be outside of the trusted domain of the users.

In untrusted storage data servers are not allowed to learn the content of sensitive data, nor can they be relied on to enforce data access policies. To keep data confidential to data servers the data owner encrypts data before upload. User access is granted by possessing the data decryption key(s) under the MA-ABE scheme. Multi Authority Attribute Based Encryption is public key cryptography for one- to-many communications. It allows the sender to specify for

DOI: 10.15680/IJIRCCE.2016. 0402079

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

each authority k a set of attributes monitored by that authority and a number dk(decryption key) so that the message can be decrypted only by a user who has at least dk of the given attributes from every authority. When this kind of attribute based access control scheme provide security protection on data. user can share their data on cloud with security using multi authority attribute based encryption.

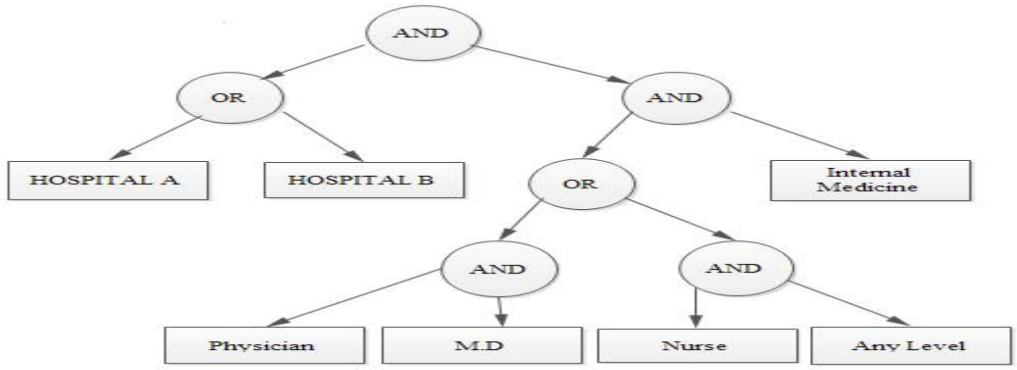

Fig .1. An Example Policy Realizable Under PHR Framework Using MA-ABE.

II.RELATED WORKS

In Role Based Access Control (RBAC) method each user access rights are determined based on his/her roles. take an example of hospital, it has many major roles such as doctor, employee, patient etc .this method allows doctor to view the entire details about the patient but, it does not allow employees to view the entire details about the patient. for employee sensitive information are hidden. In RBAC patient records are stored on multiple domain. To overcome this, Patient Controlled Encryption (PCE) are introduced. It allows the patient to selectively share their records among doctors and healthcare providers. Here, patient is fully responsible for sharing and key generation. For this reason privacy loss are occurred. Hierarchical Identity Based Encryption (HIBE) are used to separate the data from original data which contain complex information . HIBE allows the length of the cipher text to be minimized and permits the creation of escrow shelter that limit the scope of the key escrow. The scalability of the systems are achieved by Key Policy Attribute Based Encryption (KP-ABE). KP-ABE is a public key cryptography primitive for one-to-many communications. In KP-ABE, data are associated with attributes for each of which a public key component is defined. The encrypt or associates the set of attributes to the message by encrypting it with the corresponding public key components. Each user is assigned an access structure which is usually defined as an access tree over data attributes, i.e., interior nodes of the access tree are threshold gates and leaf nodes are associated with attribute. 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. For fine grained access control Ciphertext Policy Attribute Based Encryption (CP-ABE) are used. In CP-ABE private keys are labeled with a set of attributes and the ciphertexts are associated with access structures that control which user is able to decrypt the ciphertext. Moreover, CP-ABE is resistant to collusion attacks from unauthorized users. All these nice properties make CP-ABE extremely suitable for fine-grained data access control on untrusted storage.

III.EXISTING SYSTEM

In the existing system , the process uses revocable ABE algorithm. For each patient, the Patient Health Records (PHR) data should be encrypted so that it is scalable with the number of users having access. Also, since There are multiple owners (patient) in a PHR system and every owner would encrypt his/her PHR files using a different set of cryptographic key , 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. By using this techniques encrypted data can be kept confidential even if the storage is in untrusted Cloud server. Previous Attribute Based Encryption systems used attributes to describe the encrypted data and built policies into user’s keys; while in this

DOI: 10.15680/IJIRCCE.2016. 0402079

system attributes are used to describe a user's credentials, and a party encrypting data determines a policy for who can decrypt. Thus this methods are conceptually closer to traditional access control methods such as Role-Based Access Control (RBAC).In this work, just consider the setting where ciphertexts are associated with sets of policies, whereas user secret keys are associated with attributes. CP-ABE systems that allow for complex policies (like those considered here) would have a number of applications.

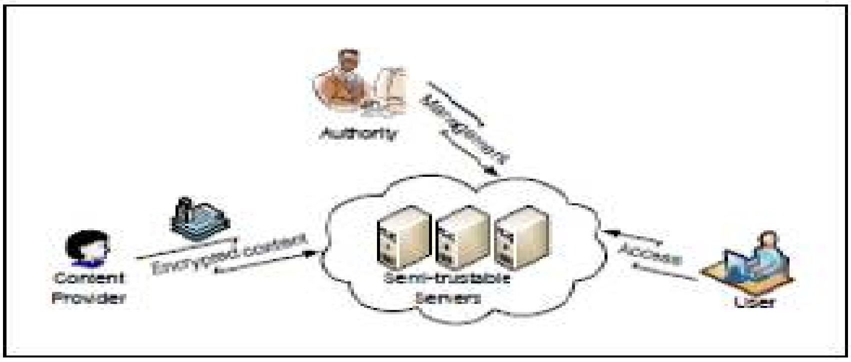

Fig.2: An Example Application Scenario of Data Sharing

An important example is a kind of sophisticated Broadcast Encryption, where users are described by (and therefore associated with) various attributes. Then, one could create a ciphertext that can be opened only if the attributes of a user match a policy. For instance, in a military setting, one could broadcast a message that is meant to be read only by users who have a rank of higher.

IV. DATA SHARING WITH DOMAIN SEPARATION

Patient Health Records (PHR) are stored at third party servers such as cloud provider. So that first generate trusted server then it classified into two domains, one for public domain and another for personal domain. Both domains are separated according to the user data access requirements. The major use of this domains for security and key management.

A. Fine grained access control vs scalability

Disclosure of sensitive data usually requires fine-grained access control in the sense that different users may have access privileges to different types/sets of data. However, ACL-based and capability-based access control, when enforced with cryptographic methods, has the scalability issue. There are several recent work [4-5], in the areas of "shared cryptographic file systems" and "access control of outsourced data" addressing the similar issue of data access control with conventional symmetric-key cryptography or public-key cryptography. When these techniques are suitable for conventional file systems, most of them are less suitable for fine-grained data access control in large-scale data centres' which may have a large number users and data files. Attribute-based encryption (ABE) [6-8], a recently invented one to- many public-key cryptography, has the potential to enforce the fine-grained access policies for large-scale systems.

B. User dynamics

An effective and efficient user management mechanism should be in place to deal with user access privilege grant and revocation. Existing solutions [6-9], suggest associating expiration time attributes to user secret keys. When these types of solutions are able to revoke user secret keys at the designated time. However, it is more suitable for real-time communication than data/file storage.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

C. Privacy preservation

As the data storage servers cannot be trusted; it is desirable to disclose as less user privacy information as possible to servers like to keep her access policy information confidential to servers and users may besides data confidentiality. In particular, the data owner would have concerns on disclosing their access privilege information to servers.

1. *User access privilege confidentiality*

This method just discloses the leaf node information of a user access tree to Cloud Servers. As interior nodes of an access tree can be any threshold gates and are unknown to Cloud Servers, it is hard for Cloud Servers to recover the access structure and thus derive user access privilege information.

2. Domain Separation

After generate trusted server domains are classified into two such as public domain and personal domain. Both domains are separated according to the user data access requirements. The major use of this domains for security and key management.

2.1) Multi Authority Attribute Based Encryption

Multi Authority Attribute Based Encryption is public key cryptography for one- to-many communications. It allows the sender to specify for each authority k a set of attributes monitored by that authority and a number dk(decryption key) so that the message can be decrypted only by a user who has at least dk of the given attributes from every authority.

2.2) Key Policy Attribute Based Encryption

Key Policy-ABE is a public key cryptography primitive for one-to-many communications. In KP-ABE ,data are associated with labels which enclose the attributes for each of which a public key component is defined. The encrypt or associates the set of attributes to the message by encrypting it with the corresponding public key components.

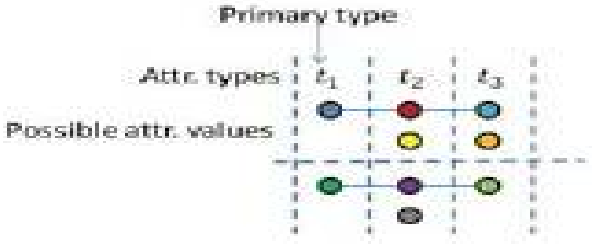

Fig. 3. Illustration of the enhanced key-policy generation rule.

3. MA-ABE for User Revocation

MA-ABE scheme enables efficient and on-demand user revocation. In particular, an authority can revoke a user or user's attributes immediately by re-encrypting the ciphertexts and updating users' secret keys, while a major part of these operations can be delegated to the server which enhances efficiency. It has nine algorithms, where MinimalSet, ReKeyGen, ReEnc and Key Update are related to user revocation, and Policy Update is for handling dynamic policy changes. A version number is used to record and differentiate the system states (*PK*, *MK*, *SK*, *CT*) after each revocation operation.

3.1) Enforce Write Access Control

If there is no restrictions on write access, anyone may write to someone's PHR using only public keys, which is undesirable. By granting write access, we mean a data contributor should obtain proper authorization from the organization she is in (and/or from the targeting owner), which shall be able to be verified by the server who grants/ rejects write access. The observation is that, it is desirable and practical to authorize according to time periods whose granularity can be adjusted.

3.2) Handle Dynamic Policy Changes

MA-ABE scheme should support the dynamic add/modify/delete of part of the document access policies or data attributes by the owner. Adding and modification of attributes/ access policies can be done by proxy re-encryption techniques[11].

3.3) Deal With Break-glass Access

For certain parts of the PHR data, medical staffs need to have temporary access when an emergency happens to a patient, who may become unconscious and is unable to change her access policies beforehand. The medical staffs will need some temporary authorization (e.g., emergency key) to decrypt those data. Under our framework, this can be naturally achieved by letting each patient delegate her emergency key to an emergency department (ED). Specifically, in the beginning, each owner defines an "emergency" attribute and builds it into the PSD part of the ciphertext of each PHR document that she allows break-glass access.

4. Security Analysis

This module analyzes the security of the proposed PHR sharing solution. It achieves data confidentiality (i.e., preventing unauthorized read accesses), by proving the enhanced MA-ABE scheme (with efficient revocation) to be secure under the attribute based selective-set model. This framework also achieves forward secrecy, and security of write access control. In addition, the proposed framework specifically addresses the access requirements in cloud-based health record management systems by logically dividing the system into PUD and PSDs, which considers both personal and professional PHR users. Our revocation methods for ABE in both types of domains are consistent. The RNS scheme only applies to the PUD.

5. Data Confidentiality

The enhanced MA-ABE scheme guarantees data confidentiality of the PHR data against unauthorized users and the curious cloud service provider, by maintaining the collusion resistance against users.

V. CONCLUSION

In earlier system, there are many challenges in maintaining the patient-centric model of health information exchange which is often outsourced to be stored at a third party, such as cloud providers. These systems has various limitations such as risk of privacy exposure, scalability in key management, flexible access and efficient user revocation, have remained the most important challenges toward achieving fine-grained, cryptographically enforced data access control. To overcome these problems, a novel patient-centric framework is proposed. It divides the customer's PHR information into multiple access domain by generating distinct key to the corresponding domain by using the Key Policy Attribute Based Encryption and Multi Authority Attribute Based Encryption. By using this technique, security and scalability of patient PHR records are expected to be achieve in an efficient manner.

REFERENCES

[1] M .Li, S. Yu, Y. Zheng, "*Scalable and Secure Sharing of Personal Health Records in Cloud Computing usingAttribute-based Encryption*"in IEEE Mar 2012.

[2] J. Anderson,"Computer Security Technology Planning Study", Air Force Electronic Systems Division, Report ESDTR- 73-51, 1972.

DOI: 10.15680/IJIRCCE.2016. 0402079

[3] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, M. Zaharia,"*Above the clouds: A berkeley view of cloud computing*", University of California, Berkeley, Tech. Rep. USB-EECS-2009-28, Feb 2009.
[4] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, K. Fu,"*Scalable secure file sharing on untrusted storage*", in Proc. of FAST'03, 2003.
[5] S. D. C. di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, P. Samarati,"*Over-encryption: Management of access control evolution on outsourced data*", in Proc. of VLDB'07, 2007.
[6] J. Bethencourt, A. Sahai, B. Waters,"*Ciphertext-Policy Attribute-Based Encryption*", In Proc. of SP'07, 2007.
[7] V. Goyal, O. Pandey, A. Sahai, B. Waters,"*Attribute-Based Encryption for Fine-grained Access Control of Encrypted Data"*, In Proc. of CCS'06, 2006.
[8] A. Boldyreva, V. Goyal, V. Kumar ,"*Identity-based Encryption with Efficient Revocation"*, In Proc. of CCS'08, 2008.
[09]S. Yu, C. Wang, K. Ren, and W. Lou, "*Attribute based data sharing with attribute revocation*," in ASIACCS'10, 2010.
[10] X. Liang, R. Lu, X. Lin, and X. S. Shen, "*Ciphertext policy attribute based encryption with efficient revocation*," Technical Report, University of Waterloo, 2010.