iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 3 **Issue:** I **Month of publication:** January 2015

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Privacy Preserving Data Sharing with CP-ABE

Neeta S. Nipane[#1], Nutan M. Dhande[*2]
[#]CSE Department, RTMNU University

Abstract*— With the recent adoption and diffusion of the data sharing paradigm in distributed systems such as online social networks or cloud computing, there have been increasing demands and concerns for distributed data security. One of the most challenging issues in data sharing systems is the enforcement of access policies and the support of policies updates. With the development of cryptography, the attribute-based encryption (ABE) draws widespread attention of the researchers in recent years. The ABE scheme, which belongs to the public key encryption mechanism, takes attributes as public key and associates them with the ciphertext or the user's secret key. It is an efficient way to solve open problems in access control scenarios, for example, how to provide data confidentiality and expressive access control at the same time. Ciphertext policy attribute-based encryption (CP-ABE) is becoming a promising cryptographic solution to this issue. It enables data owners to define their own access policies over user attributes and enforce the policies on the data to be distributed. Therefore, in this study, we propose a novel CP-ABE scheme for a data sharing system by exploiting the characteristic of the system architecture. The proposed scheme features the following achievements: 1) the key escrow problem could be solved by escrow-free key issuing protocol, which is constructed using the secure two-party computation between the key generation center and the data-storing center, and 2) fine-grained user revocation per each attribute could be done by proxy encryption which takes advantage of the selective attribute group key distribution on top of the ABE. The performance and security analyses indicate that the proposed scheme is efficient to securely manage the data distributed in the data sharing system.
Keywords*— Data sharing, attribute-based encryption, revocation, access control, removing escrow

I. INTRODUCTION

Recent development of the network and computing technology enables many people to easily share their data with others uses online external storages. With the development of the Internet and the distributed computing technology, there is a growing demand for data sharing and processing in an open distributed computing environment. People can share their lives with friends by uploading their private photos or messages into the online social networks such as Facebook and MySpace; or upload highly sensitive personal health records (PHRs) into online data servers such as Microsoft HealthVault, Google Health for ease of sharing with their primary doctors or for cost saving. The popularity of internet as a communication medium whether for personal or business use depends in part on its support for anonymous communication. As people enjoy the advantages of these new technologies and services, their concerns about data security and access control also arise. People would like to make their sensitive or private data only accessible to the authorized people with credentials they specified. Improper use of the data by the storage server or unauthorized access by outside users could be potential threats to their data. The data provider needs to provide expressive access control and data confidentiality when communicating with customers. The data outsourced to service providers are largely consumed by wide variety of individuals. Hence the need of security and privacy is an important issue. The privacy mechanism protects the sensitive attributes. This brings the idea of encrypting the data before outsourcing to the servers. However, the privacy of the shared data becoming a challenging issue [1].

Attribute-based encryption (ABE) is a promising cryptographic approach that achieves a fine-grained data access control. It provides a way of defining access policies based on different attributes of the requester, environment, or the data object. Especially, ciphertext policy attribute-based encryption (CP-ABE) enables an encryptor to define the attribute set over a universe of attributes that a decryptor needs to possess in order to decrypt the ciphertext, and enforce it on the contents. Thus, each user with a different set of attributes is allowed to decrypt different pieces of data per the security policy. This effectively eliminates the need to rely on the data storage server for preventing unauthorized data access. Data sharing or information sharing is necessary for distributed systems. These records should be maintained with privacy and security for safe retrieval. The privacy mechanism protects the sensitive attributes. The security schemes are used to protect the data from public access. The data are allowed to be accessed only by authorized individuals. Each party is assigned with access permission for a set of attributes. The attribute based encryption scheme is enhanced to handle distributed attribute based encryption process. Data update and key management operations are tuned for multi user access environment.

II. LITERATURRE REVIEW

ABE comes in two flavors called key-policy ABE (KP-ABE) and ciphertext-policy ABE (CP-ABE). In KP-ABE, attributes are used to describe the encrypted data and policies are built into users' keys; while in CP-ABE, the attributes are used to describe users' credentials, and an encryptor determines a policy on who can decrypt the data. Between the two approaches, CP-ABE is

more appropriate to the data sharing system because it puts the access policy decisions in the hands of the data owners. Most of the existing ABE schemes are constructed on the architecture where a single trusted authority, or KGC has the power to generate the whole private keys of users with its master secret information. Thus, the key escrow problem is inherent such that the KGC can decrypt every ciphertext addressed to users in the system by generating their secret keys at any time.

Junbeom Hur [1], proposed CP-ABE schemes with slight changes in attribute rather than from the scratch and remove the problem which is encountered in Bethencourt et al. [5], like key escrow and revocation. But in this system there is computational overhead.

M. Chase and S.S.M. Chow [2], proposed a distributed KP-ABE scheme that solves the key escrow problem in a multi-authority system. Most of the existing ABE schemes are constructed on the architecture where a single trusted authority, or KGC has the power to generate the whole private keys of users with its master secret information. Thus, the key escrow problem is inherent such that the KGC can decrypt every ciphertext addressed to users in the system by generating their secret keys at any time. One disadvantage of this kind of fully distributed approach is the performance degradation.

S.S.M. Chow [3], proposed an anonymous private key generation protocol in identity-based literature such that the KGC can issue a private key to an authenticated user without knowing the list of users' identities. However, found that this cannot be adapted to ABE systems due to mainly two reasons. First, in Chow's protocol, identities of users are not public anymore, at least to the KGC, because the KGC can generate users' secret keys otherwise. Second, the collusion attack between users is the main security threat in ABE.

J. Bethencourt, A. Sahai, and B. Waters [4], and A. Boldyreva, V. Goyal, and V. Kumar [5], proposed first key revocation mechanisms in CP-ABE and KP-ABE settings, respectively. These schemes enable an attribute key revocation by encrypting the message to the attribute set with its validation time. These attribute-revocable ABE have the security degradation problem in terms of the backward and forward secrecy.

N. Attrapadung and H. Imai [6], suggested another user-revocable ABE schemes addressing the key revocation problem by combining broadcast encryption schemes with ABE schemes. However, in this scheme, the data owner should take full charge of maintaining all the membership lists for each attribute group to enable the direct user revocation. This scheme is not applicable to the data sharing system, because the data owners will no longer be directly in control of data after storing their data to the external storage server.

S. Yu, C. Wang, K. Ren, and W. Lou [7], recently addressed the user revocation in the ABE-based data sharing system. In this scheme, the user revocation is realized using proxy reencryption by the data server. However, in order to revoke users, the KGC should generate all secret keys including the proxy key on behalf of the data server. Then, the server would reencrypt the ciphertext under the proxy key received from the KGC to prevent revoked users from decrypting the ciphertext. Thus, the key escrow problem is also inherent in this scheme.

S. D. C. di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. Samarati [8], proposed a solution for securing outsourced data on semi-trusted servers based on symmetric key derivation methods which can achieve fine-grained access control. Unfortunately, the complexities of file creation and user grant/revocation operations are linear to the number of authorized users, which is less scalable.

Shilpa Elsa Abraham and R. Gokulavanan [10], proposed The system scalability is enhanced using ABE and MA-ABE. The expressibility of our encryptor's access policy is somewhat limited by that of MA-ABE's. In practice, the credentials from different organizations may be considered equally effective, in that case distributed ABE schemes will be needed. The following drawbacks are identifying from the existing system. User identity bases access control mechanism is not supported under the situation. Dynamic policy management is yet another issue.

III.SECURITY ANALYSIS OF THE PROPOSED SYSTEM

According to the existing schemes, the functionalities in an ideal ABE scheme is listed as follows:

Data confidentiality: Unauthorized participants cannot know the information about the encrypted data.

Fine-grained data access control: In order to achieve flexible access control, even for users in the same group, their access rights are not the same.

User/attribute revocation: If a user quits the system, the scheme can revoke his access right. Similarly, attribute revocation is inevitable.

Collusion resistance: The dishonest users cannot combine their attributes to decrypt the encrypted data.

Scalability: The number of authorized users cannot affect the performance of the scheme. That is to say, the scheme can deal with the case that the number of the authorized users increases dynamically.

IV. PROPOSED METHODOLOGY

The first CP-ABE scheme proposed by Bethencourt et al. [4], which are mostly motivated by more rigorous security proof in the standard model. However, most of the schemes failed to achieve the expressiveness of the Bethencourt et al.'s scheme. Therefore, in this proposed, develop a variation of the CP-ABE algorithm partially based on (but not limited to) Bethencourt et al.'s construction in order to enhance the expressiveness of the access control policy instead of building a new CP-ABE scheme from scratch. The attribute based encryption scheme is enhanced to handle distributed attribute based encryption process. Data update and key management operations are tuned for multi user access environment.

Its key generation procedure is modified for removing key escrow. The proposed scheme is then built on this new CP-ABE variation by further integrating it into the proxy reencryption protocol for the user revocation. To handle the fine-grained user revocation, the data storing center must obtain the user access (or revocation) list for each attribute group, since otherwise revocation cannot take effect after all. This setting where the data-storing center knows the revocation list does not violate the security requirements, because it is only allowed to reencrypt the ciphertexts and can by no means obtain any information about the attribute keys of users. The two parties engage in the arithmetic 2PC protocol with master secret keys of their own, and issue independent key components to users during the key issuing phase. The 2PC protocol deters them from knowing each other's master secrets so that none of them can generate the whole set of secret keys of users individually. Thus, we take an assumption that the KGC does not collude with the data-storing center since they are honest.

A. Data Sharing Architecture

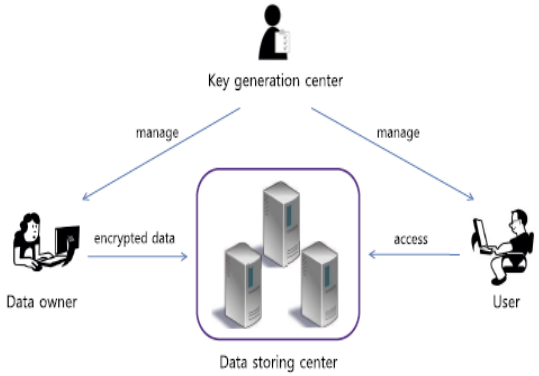


Fig.1 Architecture of data sharing system

Fig.1 shows the architecture of the data sharing system, which consists of the following system entities:

1) *Key generation center:* It is a key authority that generates public and secret parameters for CP-ABE. It is in charge of issuing, revoking, and updating attribute keys for users. It grants differential access rights to individual users based on their attributes. That is, it will honestly execute the assigned tasks in the system; however, it would like to learn information of encrypted contents as much as possible. Thus, it should be prevented from accessing the plaintext of the encrypted data even if it is honest.
2) *Data-storing center:* It is an entity that provides a data sharing service. It is in charge of controlling the accesses from outside users to the storing data and providing corresponding contents services. The data-storing center is another key authority that generates personalized user key with the KGC, and issues and revokes attribute group keys to valid users per each attribute, which are used to enforce a fine-grained user access control.
3) *Data owner:* It is a client who owns data, and wishes to upload it into the external data-storing center for ease of sharing or for cost saving. A data owner is responsible for defining (attribute-based) access policy, and enforcing it on its own data by encrypting the data under the policy before distributing it.
4) *User:* It is an entity who wants to access the data. If a user possesses a set of attributes satisfying the access policy of the encrypted data, and is not revoked in any of the valid attribute groups, then he will be able to decrypt the ciphertext and obtain the data.

B. Advantages

1) Distributed environment
2) Security of sensitive fields

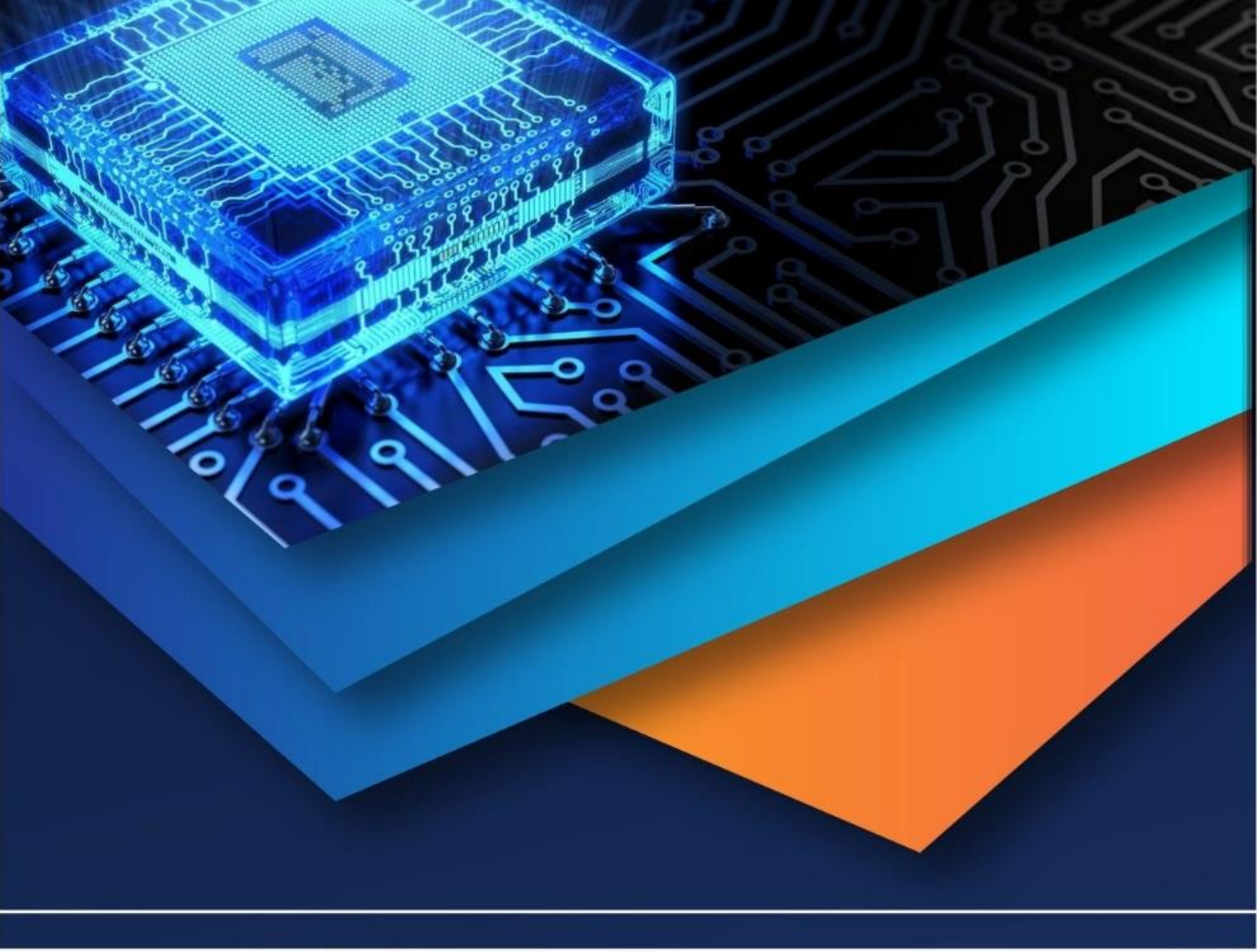
3) Break glass access for emergency situations
4) On-demand revocation

V. CONCLUSIONS

A novel framework of secure sharing of personal records under distributed environment with the CP-ABE encryption technique has been proposed in this paper . Public and personal access models are designed with security and privacy enabled mechanism. The framework addresses the unique challenges brought by multiple transaction records of owners and users, in that the complexity of key management is greatly reduced while guaranteeing the privacy compared with previous works. The attribute-based encryption model is enhanced to support distributed ABE operations with CP-ABE. The system is improved to support dynamic policy management model.

REFERENCES

[1] Junbeom Hur, "Improving Security and Efficiency in Attribute-Based Data Sharing" *IEEE Transactions On Knowledge And Data Engineering* Vol:25 No:10 Year 2013
[2] M. Chase and S.S.M. Chow, "Improving Privacy and Security in Multi-Authority Attribute-Based Encryption," *Proc. ACM Conf. Computer and Comm. Security*, pp. 121-130, 2009.
[3] S.S.M. Chow, "Removing Escrow from Identity-Based Encryption," *Proc. Int'l Conf. Practice and Theory in Public Key Cryptography (PKC '09),* pp. 256-276, 2009.
[4] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-Policy Attribute-Based Encryption," *Proc. IEEE Symp. Security and Privacy,* pp. 321-334, 2007.
[5] A. Boldyreva, V. Goyal, and V. Kumar, "Identity-Based Encryption with Efficient Revocation," *Proc. ACM Conf. Computer and Comm. Security,* pp. 417-426, 2008.
[6] N. Attrapadung and H. Imai, "Conjunctive Broadcast and Attribute-Based Encryption," *Proc. Int'l Conf. Palo Alto on Pairing-Based Cryptography (Pairing),* pp. 248-265, 2009.
[7] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute Based Data Sharing with Attribute Revocation," Proc. ACM Symp. Information, Computer and Comm. Security (ASIACCS '10), 2010.
[8] S. D. C. di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. Samarati, "Overencryption: management of access control evolution on outsourced data," in VLDB '07, 2007, pp. 123–131.
[9] Shilpa Elsa Abraham and R. Gokulavanan "Ensuring Privacy and Security in Data Sharing under Cloud Environment" *International Journal of Computer Applications Technology and Research Volume 2– Issue 2,* 188 - 194, 2013



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY