IMPROVING SECURITY AND PRIVACY ATTRIBUTE BASED DATA SHARING IN CLOUD COMPUTING

B. Uma Maheswari[1], K. Siri Chandana[2]

[1]Assistant Professor, Dept. of MCA, Audisankara College of Engineering and Technology (AUTONOMOUS), Gudur, AP, India.

[2]PG Scholar, Dept. of MCA, Audisankara College of Engineering and Technology (AUTONOMOUS), Gudur, AP, India.

ABSTRACT

Data sharing is a convenient and economic service supplied by cloud computing. Data contents privacy also emerges from it since the data is outsourced to some cloud servers. To protect the valuable and sensitive information, various techniques are used to enhance access control on the shared data. In these techniques, Cipher-text policy attribute-based encryption (CP-ABE) can make it more convenient and secure. Traditional CP-ABE focuses on data confidentiality merely while the user's personal privacy protection is an important issue at present. CP-ABE with hidden access policy ensures data confidentiality and guarantees that user's privacy is not revealed as well. However, most of the existing schemes are inefficient in communication overhead and computation cost. Moreover, most of those works take no consideration on authority verification or the problem of privacy leakage in authority verification phase. To tackle the problems mentioned above, a privacy preserving CP-ABE scheme with efficient authority verification is introduced in this paper. Additionally, the secret keys of it achieve constant size. Meanwhile, the proposed scheme achieves the selective security under the decisional n-BDHE problem and decisional linear assumption.

I. INTRODUCTION

To maintain data integrity on the cloud, Attribute-based Encryption (ABE) with Key Policy Attribute based Encryption (KP-ABE) and Cipher text-Policy Attribute-based Encryption (CP-ABE) can be used with access control implementation for cloud computing. CP-ABE is a promising cryptographic primitive for secure data sharing in cloud computing. A data owner is the only charge of to define the access policy associated with his data which to be shared. In CP-ABE, each user's secret keys are associated with a set of attributes and data are encrypted with access policy on attributes. A user can decrypt a cipher-text if and only if his attributes satisfy the cipher-text access policy. In CP-ABE, the secret keys of users have to be issued by a trusted key authority that leads to key escrow problem. Besides, most of the existing CPABE schemes cannot support attribute with an arbitrary state. In this paper, weighted attribute data sharing scheme is proposed to solve the key escrow problem and also improve the expressiveness of attribute, so that the resulting scheme is friendlier to cloud computing applications. An improved two-party key issuing protocol guarantees that neither key authority nor cloud service provider can compromise the whole secret key of a user individually. The concept of weighted attribute not only enhance the expression of an attribute binary to arbitrary but also reduce the complexity of access policy, so that storage cost of cipher-text and time cost in encryption can be reduced Therefore, the data owner requires high security and confidentiality of the data when outsourcing it in the cloud. However, traditional cryptographic primitives cannot be directly employed to achieve data security. Recently, there has been a plethora of work on privacy and security in the content of ensuring sharing of remotely stored data under different systems and security models [2], [3], [4].

Those works mainly focus on how to preserve the user's privacy and realize the desired security goal without bringing a high complexity on the user decrypted stage. To solve this issue, researchers either utilize key-policy attribute-based encryption (KP-ABE) for secure access control, or employ hierarchical identity based encryption (HIBE) for data security. The KP-ABE-based this work is supported in part by the National Key Basic Research and Development Plan of China under Grant 2013AAOIA601. The National Natural Science Foundation of China under Grant 61170237. and the Doctoral Program of Higher Education of China however, reveal some users access attributes to the cloud, and then these cannot fully preserve the user's privacy and are also not fully collusion resistant. On the other hand, the HIBE-based schemes [4], introduce too many keys (each user has a mass of keys) and cannot manage efficiently. Therefore, the challenge to achieve goals of both privacy preserving and effective cloud data sharing service still remains open. To realize an effective and privacy-preserving data sharing service in cloud computing, the following requirements should be achieved. Firstly, the data owner should be able to decide whether a user can access to his cloud data or not. Secondly, the privacy of users should be protected against the cloud. Finally, the accessing users may access the sharing data using connected terminals with low computing ability, such as smart phone and tablet. To date, these important fields in cloud sharing remains elusive. In this paper, we address these issues and propose an effective and flexible privacy-preserving data sharing scheme, P2E. To preserve privacy and guarantee the data confidentiality against the cloud, we employ a cryptographic primitive, named cipher-text policy attribute-based encryption (CP-ABE), combined it with the technique of identity based encryption (IBE). Compared with KPABE-based schemes, P2E introduces user public key which is tight with user secret key to realize fully collusion secure and privacy preserving. Meanwhile, P2E does not increase user keys so as to reduce the key management issues compared with HIBE-based schemes. P2E describes each data file with a set of meaningful attributes and assigns an access structure to these attributes for each user that reflects the scope of data files the user is allowed to access. When combined with each user's public key, the secret key of the same attribute for different users differs. To enforce these access structures, we define a public/secret key pair for each attribute. Data files are encrypted by public key components and access matrices converted from the access structure. User secret keys are defined to reflect their access privileges so that a user is able to decrypt a cipher-text only if he has the matched attributes to satisfy the cipher-text. Specifically, the main contributions of this paper can be summarized as following: 1) We propose an effective privacy-preserving encryption scheme P2E that simultaneously achieves full privacy preserving, collusion resistance and data confidentiality for cloud data sharing service; 2) We prove that P2E is secure and P2E also simultaneously enforces fine-graininess, backward secrecy and access privilege confidentiality for data sharing in cloud computing; 3) The performance analysis indicates that incurs only a small overhead compared to the existing works. Meanwhile, the experiment results demonstrate P2E is as light as possible.

II. LITERATURE SURVEY

ABE schemes specify two kinds of policies, the key policy (KP) and the cipher-text policy (CP), which result in a KP-ABE and a CP-ABE, respectively. In a KP-ABE scheme, the private key is generated under a specified access policy, while in a CP-ABE scheme; the cipher-text is related to a specified access policy. Only users whose attributes match the policy can recover data successfully. Now ABE has been a hot research area [3]–[7]. However, most of them take only the data confidentiality into consideration while ignoring the importance of user privacy preserving. The first work with consideration of user personal privacy was introduced by Nishide et al. [8], where the access policy was partially hidden by dividing attribute into two parts as value and name, while only hiding the value. Due to the hidden policy, the adversary cannot get any information about the users. However, their scheme is impractical since its computation cost is too high.

In 2009, Waters proposed a CP-ABE scheme with dual system encryption technique [7]. It provided a new way for privacy preserving in CP-ABE. Then Lai et al. [9], [10] used this technique to issue two hidden access policy CP-ABE schemes (HP-CP-ABE). Both of them have been proven to achieve full security. The first one [9] only supports AND gate, and the second one [10] supports linear secret share scheme (LSSS) [11], which is a more expressive access structure. However, the size of both secret keys and cipher-text increases linearly with the number of attributes. Then Rao et al. [12] introduced another HP-CP-ABE scheme with full security. In this scheme, its security also relies on composite-order group, but the size of secret keys and cipher-text achieves constant which improves the efficiency compared with [9] and [10]. However, this scheme only supports AND gate, which is not expressive.

Zhang et al. [13] proposed a hierarchical HP-CP-ABE scheme, where they used the technique proposed by Abdalla et al. [14]. It achieves constant size secret keys and supplies fast decryption. Recently, Huang et al. [15] presented an HP-CP-ABE with lower computation cost and constant size secret keys. However, it only achieves selective security, which is not a strong enough security model. Although the above mentioned schemes can protect users' privacy, there is an important problem to be ignored. That is to say, if the access policy is hidden, the users have to attempt the entire possible combinations of the secret keys to decrypt the cipher-texts, which mean the users must take more time to recover messages. It is necessary to find a method to help the users decrypt cipher-texts efficiently and successfully. To address this problem, Zhang et al. [16] introduced an HP-CP-ABE scheme with authority verification phase to decrease users' computational consumption. The authority verification phase can help users check whether they are the valid users or not. However, privacy leakage is found in the match phase.

Then Li et al. [17] proposed a more efficient HP-CP-ABE scheme with authority verification. It can decrease users' unnecessary computational consumption. However, the same problem with [16], attributes in access policy can also be tested out in authority verification phase. Cui et al. [18] introduced another HP-CP-ABE scheme. But the size of secret keys and cipher-texts are both increasing with the number of attributes. Recently, Khan et al. [19] proposed an HP-CPABE scheme with LSSS access structure. And it also supports authority verification. However, they employed hidden vector encryption to achieve this. It is not efficient enough, relatively. Zhang et al. [20] presented an HP-CP-ABE scheme, where it supports large universe attribute set and LSSS access policy. However it is based on Composite order group, which is inefficient than the schemes based on prime order group in the same case. Another technique supporting hidden access policy comes from inner-product predicate encryption (IPE) [21], [22]. However, this conversion will generate a great loss in efficiency. An instance based on IPE due to Phuong et al. [23] shows that the size of secret keys and cipher-texts in this scheme increases linearly with the depth of attributes, which takes more storage and computational resource.

III. PROPOSED SYSTEM

We introduce an HP-CP-ABE scheme supporting efficient authority identification, which is used to help the user determine whether he/she is authorized or not. The test technique comes from the Abdalla’s verifiable random functions with the auxiliary information, where the auxiliary information is used to generate the test parameters. The proposed scheme can solve the cipher-texts verification without disclosing the privacy of the users.

A framework of HP-CP-ABE with efficient authority identification is proposed, which guarantees the data confidentiality and protects the user personal privacy as well. In order to avoid unnecessary computations of users in decryption algorithm, we design an authority identification method, which can help the user verify whether he/she is an authorized one and decrypts successfully.

The proposed scheme achieves constant private key size, which is independent of user’s attribute number. It reduces the cost of transmission and storage. In addition, a compact security analysis by using a sequence of hybrid games is given to show the proposed scheme of how to achieve anonymity, which is lacking in most of the existing works.

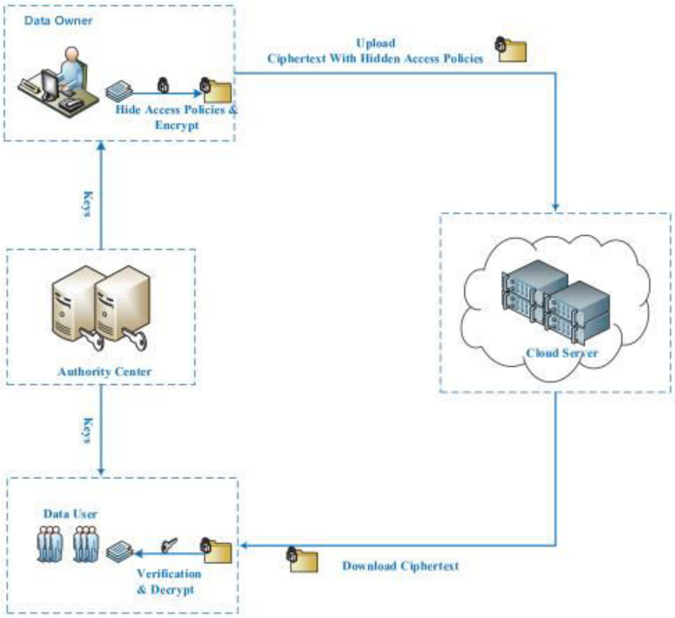

Fig: Architecture of the proposed methodology

SYSTEM MODEL AND FRAMEWORK

1) System Model: There are four entities in a HP CP-ABE system: A CS, an authority center (AC), DO, and data users (DU) as shown in Fig.

1) AC: In the HP-CP-ABE, it should be fully trusted and accepts the registration of all DU. then it will generate public keys and secret keys for each DU.

2) DO: DO specify access policies and encrypts data. Then he/she uploads the encrypted data to the CS.

3) CS: CS may not be honest in the system. It is in charge of storing encrypted data.

4) DU: DU can request secret keys associated with their attributes from AC and access to encrypted data from CS. If DU can pass the verification, which means their attributes match the policy, then DU can recover the encrypted contents

VI. CONCLUSION

We proposed a privacy preserving CP-ABE scheme in the standard model. The presented scheme has many advantages over the existing schemes, such as constant size private keys and short cipher-texts. And in decryption, it only needs four pairing computations. The proposed scheme achieves selective security and anonymity in a prime order group. In the standard model, we show the security of the proposed scheme is reduced to the decisional n-BDHE and the DL assumptions. Additionally, the proposed scheme supports authority verification with no privacy leakage. However, the introduced scheme only supports "AND" policy and relies on a weak security model. How to construct a strong secure HP-CP-ABE scheme with more flexible access policy is left for the future works.

V. REFERENCES

[1] P. P. Kumar, P. S. Kumar, and P. J. A. Alphonse, "Attribute based encryption in cloud computing: A survey, gap analysis, and future directions," J. Netw. Comput. Appl., vol. 108, pp. 37–52, 2018.

[2] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Proc. 24th Annu. Int. Conf. Theory Applications Cryptographic Techn., May 2005, vol. LNCS 3494, 2015, pp. 457–473.

[3] K. Emura, A. Miyaji, A. Nomura, K. Omote, and M. Soshi, "A ciphertextpolicy attribute-based encryption scheme with constant ciphertext length," in Proc. 5th Int. Conf. Inf. Security Practice Experience, Apr. 2009, pp. 13– 23.

[4] J. Han, W. Susilo, Y. Mu, and J. Yan, "Privacy-preserving decentralized key-policy attribute-based Encryption," IEEE Trans. Parallel Distrib. Syst., vol. 23, no. 11, pp. 2150–2162, Nov. 2012.

[5] S. Wang, J. Zhou, J. K. Liu, J. Yu, J. Chen, and W. Xie, "An efficient file hierarchy attribute-based encryption scheme in cloud computing," IEEE Trans. Inf. Forensics Secur., vol. 11, no. 6, pp. 1256–1277, Jun. 2016.

[6] A. Lewko and B. Waters, “Decentralizing attribute-based encryption,” in Proc. 30th Annu. Int. Conf. Theory Appl. Cryptographic Techn.: Advances Cryptology, May 2011, pp. 568–588.

[7] B. Waters, “Dual system encryption: Realizing fully secure IBE and HIBE under simple assumptions,” in Proc. 29th Annu. Int. Cryptology Conf. Advances Cryptology, Aug. 2009, pp. 619–636.

[8] T. Nishide, K. Yoneyama, and K. Ohta, “Attribute-based encryption with partially hidden encryptor-specified access structures,” in Proc. Appl. Cryptogr. Netw. Security, Jun. 2008, vol. LNCS 5037, pp. 111–129.

[9] J. Lai, X. Zhou, R. H. Deng, and Y. Li, “Fully secure cipertext-policy hiding CP-ABE,” in Proc. 6th ACM Symp. Inf. Comput. Commun. Secur., 2011, pp. 24–39.

[10] J. Lai, X. Zhou, R. H. Deng, Y. Li, and K. Chen, “Expressive CP-ABE with partially hidden access structures,” in Proc. 7th ACM Symp. Inf. Comput. Commun. Secur., May 2012, pp. 18–19.

[11] B. Waters, “Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization,” in Proc. 14th Int. Conf. Practice Theory Public Key Cryptography Conf. Public Key Cryptography, Mar. 2011, pp 53–70.

[12] Y. S. Rao and R. Dutta, “Recipient anonymous ciphertext-policy attribute based encryption,” in Proc. 9th Int. Conf. Inf. Sys. Secur., Dec. 2013, pp. 329–344.

[13] L. Zhang, Q. Wu, Y. Mu, and J. Zhang, “Privacy-preserving and secure sharing of PHR in the cloud,” J. Med. Syst., vol. 40, pp. 1–13, 2016.

[14] M. Abdalla, D. Catalano, and D. Fiore,“Verifiable random functions: Relations to identity-based key encapsulation and new constructions,” J. Cryptol., vol. 27, pp. 544–593, 2014.

[15] C. Huang, K. Yan, S. Wei, G. Zhang, and D. H. Lee, “Efficient anonymous attribute-based encryption with access policy hidden for cloud computing,” in Proc. IEEE Int. Conf. Progress Inform. Comput., Dec. 2017, pp. 266– 270.

AUTHOR'S PROFILE

B. UMA MAHESWARI is currently working as Assistant Professor in Audisankara College of Engineering and Technology (AUTONOMOUS), NH-5, Bypass Road, Gudur, Tirupati (Dt.), Andhra Pradesh, India.

K. SIRI CHANDANA is pursuing MCA from Audisankara College of Engineering and Technology (AUTONOMOUS), NH-5, Bypass Road, Gudur, Tirupati (Dt.), Andhra Pradesh, India.