IMPROVING SECURITY AND PRIVACY ATTRIBUTE BASED DATA SHARING IN CLOUD COMPUTING

Peteti Jaya Simha Hari, Sri.G.Ramesh Kumar, Sri.V.Bhaskara Murthy,
MCA Student, Assistant Professor, Associate Professor
Dept Of MCA
B.V.Raju College, Bhimavaram

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 about 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. The computational results confirm the merits of the presented scheme.

I. INTRODUCTION

CLOUD techniques make it possible to utilize information technology resources into business domain. The cloud provides variety of scalable services on-demand, such as online databases, program interface, storage and computing resources, etc. Users can obtain services through phones, laptops, and desktops as shown in Fig. 1. Cloud storage provides remote data storage and management services. It is also helpful in data analyzing and computing, which is quite simple as it can provide a variety of services at the same time. Cloud has many advantages in data storage, such as decreasing communication cost and maintenance charge, saving resources, allowing remote access, and so on. However, people might not be willing to store their data in the cloud, even though it provides so many benefits because of the data confidentiality and privacy problems. The cloud server (CS) may be untrusted, in other words, if data is uploaded to cloud, the cloud service provider may obtain and disclose users' personal privacy, and even access and share the
data illegally [1].

To make sure the confidentiality of the data in cloud, people are inclined to encrypt them before they are uploaded to cloud. But the general encryption algorithms make the data

process become difficult. ABE is a good candidate to overcome this limitation. ABE was first proposed in 2005 by Sahai and Waters [2], which guaranteed the data confidentiality and provided the fine-grained access control policy to the customers. It has been widely accepted as an effective method encrypting the outsourced data in cloud computing. ABE improves the efficiency when the data owner (DO) intends to share data contents with multiusers. It permits DO to specify an access policy to the encrypted files, which can make the users who match it, access uploaded data. The users who do not satisfy the access structure cannot get any information about the data contents. For instance, we consider the data access control for a company. If the CEO intends to submit a classified file, through the cloud, to the managers in sales department, planning department, and research and development (R&D) department. Then he/she can use an ABE scheme. First he/she encrypts the file and specifies an access structure as ω = manager ∧ (sales department ∨planning department ∨ R&D). Next he/she uploads the encrypted file and the access structure into the CS. Only the managers in the three mentioned departments can access the classified file, and the managers in other departments or the general staff in the three mentioned departments cannot learn anything about the file even if they collude.

Most of ABE proposals perform very well in secure data sharing. However, the personal privacy of the DO and the users is ignored in these constructions. For convenience of recovering data, the access policy is always sent with ciphertexts. In some scenarios, the access structure may carry sensitive information of users. For instance, a patient wants to share his/her personal health record (PHR) with some doctors and family members, but he/she may not want others to know that he/she is sick. If the patient employs a normal ABE scheme to encrypt the PHR, although the malicious user cannot get the contents of the PHR, he/she may get some information about the users as shown in Fig. 2. The access policy contains “cardiopathy” and “DC hospital” and the malicious third party may guess that the DO is suffering from a heart attack and is treating in the DC hospital. Hence a natural problem is how to keep the shared data secure, while the privacy of them is also protected.

II. EXISTING SYSTEM

- 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 ciphertext 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 ciphertext 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 ciphertexts, which means the users must take more time to recover messages. It is necessary to find a method to help the users decrypt ciphertexts 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.

Disadvantages

- In the existing work, system is either coarse grained or short of scalability as the number of users increases.
- The existing doesn't use 256 or 512 bit encrypted keys.

III. PROPOSED SYSTEM

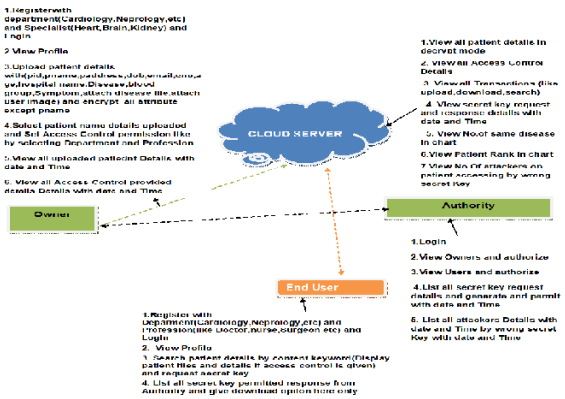
- A framework of HP-CP-ABE with efficient authority identification is proposed, which guarantees the data confidentiality and protects the user personal privacy as well.
- In order to avoid unnecessary computations of users in decryption algorithm, we design an authority identification method, which 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.

Advantages

- The system is more secure due to the data contents which have been kept confidential to unauthorized individuals and collaborating users, including the curious cloud servers.
- The system is more secured since the Users from different groups cannot decrypt the cipher text by collaboration.

IV. ARCHITECTURE DIAGRAM



V. IMPLEMENTATION

DATA OWNER

In this module, Data owner has to register to cloud and logs in, Encrypts and uploads a file to cloud server and also performs the following operations such as Register with department(Cardiology,Neprology,etc) and Specialist(Heart,Brain,Kidney) and Login and View Profile ,Upload patient details with(pid,pname,paddress,dob,email,cno,age, hospital name,Disease,blood group,Symptom,attach disease file, attach user image) and encrypt all attribute except pname ,Select patient name details uploaded and Set Access Control permission like by selecting Department and Profession and View all uploaded patient Details with date and Time ,View all Access Control provided details with date and Time.

CLOUD SERVER

In this module the cloud will authorize both the owner and the user and also performs the following operations such as View all patient details in decrypt mode and View all Access Control Details, View all Transactions (like upload, download, search) and View secret key request and response details with date and Time View No.of same disease in chart, View Patient Rank in chart and View No.Of attackers on patient accessing by wrong secret Key

Authority

In this module, the Authority performs the following operations such as Login ,view Owners and authorize and View Users and authorize,List all secret key request details and generate and permit with date and Time and List all attackers Details with date and Time by wrong secret Key with date and Time.

End USER

In this module, the user has to register to cloud and log in and performs the following operations such as Register with Deparment(Cardiology,Neprology,etc) and Profession(like Doctor,nurse,Surgeon etc) and Login ,View Profile and Search patient details by content keyword(Display patient files and details if access control is given)

and request secret key and List all secret key permitted response from Authority and give download option here only.

VI. CONCLUSIONS

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.

REFERENCES

[1] P. P.Kumar, P. S.Kumar, and P. J. A. Alphonse, "Attribute based encryption in cloud computing:Asurvey, 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.

[16] Y. Zhang, X. Chen, J. Li, D.Wong, and H. Li "Anonymous attribute-based encryption supporting efficient decryption test," in Proc. 8th ACM Symp. Inf. Comput. Commun. Secur., May 2013, pp. 511–516.

[17] J. Li, H. Wang, Y. Zhang, and J. Shen, "Ciphertext-policy attribute-based encryption with hidden access policy and testing," KSII Trans. Internet Inf. Syst., vol. 10, no. 7, pp. 3339–3352, Jul. 2016.

[18] H. Cui, R. H. Deng, G. Wu, and J. Lai, "An efficient and expressive Ciphertext-policy attribute-based encryption scheme with partially hidden access structures," in Proc. 10th Int. Conf. Prov. Secur., Nov. 2016, pp. 19–38.

[19] F. Khan, H. Li, L. Zhang, and J. Shen, "An expressive hidden access policy CP-ABE," in Proc. IEEE 2nd Int. Conf. Data Sci. Cyberspace, Jun. 2017, pp. 26–29.

[20] Y. Zhang, Z. Dong, and R. H. Deng, "Security and privacy in smart health: Efficient policy-hiding attribute-based access control," IEEE Int. Things J., vol. 5, no. 3, pp. 2130–2145, Jun. 2018.