



WEIGHTED ATTRIBUTE DATA SHARING IN CLOUD COMPUTING

T. Shashank¹, N. Vijay Kumar²

^{1,2} Computer Science, SR Engineering College,
Warangal, Telangana State, India.

vijay_kumar_n@srecwarangal.ac.in²,

shashank.t769@gmail.com¹

October 25, 2018

Abstract

Ciphertext-policy attribute-based encryption (CPABE) is a technique of encryption which is economical and safe for data sharing in cloud computing. In this technique, the owner of the data is able to manage access policy related to the data which has to be shared. But, CP-ABE has a major security drawback called as key escrow problem wherein the key authority issues secret keys of users. In this problem, Escrow denotes storage, in which storage of the key is done in third party or key generation centre. This center can decrypt any messages sent to various users by using their private keys. In this paper, an attempt has been made to revisit attribute-based data sharing scheme so as to overcome the key escrow issue and also improve the expressiveness of an attribute by adding weight, so that there is enhancement of the expression of attribute from binary to arbitrary state. Thus, the complexity of encryption and storage cost of a cipher text are reduced.

INDEX TERMS:- Attribute-based Encryption, Access control, Cloud Storage.

1 INTRODUCTION

In the present age, the usage of technology and internet has made our lives easy. Nowadays we can share any kind of data like text, image, audio and video. Cloud computing provides an easy and efficient method to store, secure and access data at any time and place with the use of internet. Trusted third parties play major role in cloud computing as they provide us secure channel for transferring the data from data owner to the particular group of users. Trusted third parties like Key authority which generate public and private keys may know these keys to steal the information related to the users and misuse it, resulting in creation of Escrow problem. These days, due to huge number of internet users, we also need to protect our data from misuse and an unauthorized person should not be able to access the private data of an individual. Hence, we have to take care of privacy of data by using Data protection techniques like attribute based encryption [1]. The main aim of our work is to provide secure sharing of data in cloud. The important factors in cloud storage include Data confidentiality and performance.

Confidentiality of Data: The plain text of the data should not be accessible to the unauthorized users Who do not have attributes to satisfy the access policy?

Fine grained access control: Access control list (ACL) is made in such a way that authorized users can only access the data by providing them with the necessary access policy.

Shamir [5] proposed the idea of Secret sharing in 1979 which shows how to share a secret among parties securely.

In 1984, Shamir presented a novel cryptographic scheme also known as Identity-Based Encryption (IBE)[6], which allows two parties to share data securely without exchanging public key or private key. In IBE scheme, data owner encrypts message with respective to IP address which is a unique identity. The user holding a specific identity can decrypt message by using identity as a key. Thus, the risk of key exposure is lessened.

The first Attribute Based Encryption scheme called fuzzy identity-based encryption technique was conceived in 2005, by Sahai and Waters [2] in which a set of descriptive attributes is considered as identity and it possesses both cipher text and recipients. Recipients who have the attribute similar to the fuzzy identity can access the

data.

The attribute-based encryption techniques are mainly of two types: cipher text-policy attribute-based encryption (CP-ABE)[4] and Key-policy attribute-based encryption (KP-ABE).[3]

Cipher text-Policy ABE

In this technique, the private-key of user is linked to a set of attributes and an access policy defined over a universe of traits is listed in the cipher text. Cipher text can be decrypted by a recipient, only when recipients attributes fully satisfy the access policy of the respective cipher text. Access policies can be made over attributes using conjunctions, disjunctions and (k,n) -threshold gates, that is k out of n attributes. For example, if the universe of attributes is defined as A,B,C,D and user 1 receives a key to attributes A,B and user 2 to attribute D then a cipher text encrypted to the access policy $(AC)D$, will enable user 2 to decrypt, while user 1 will be unable to decrypt.

In this way, inherent authorization is enforced in CP-ABE which means that encrypted data includes authorization and the data can be decrypted by users only who satisfy the particular policy.

Key-Policy ABE

This is another technique of Attribute Based Encryption. In this technique the secret key of user is encoded with access policy. For example, access policy $(AC)D$ in a ciphertext with set of attributes A,B , then user is unable to decrypt the ciphertext but is able to decrypt a ciphertext with respect to A,C .

To prevent, users from pooling their secret keys to decrypt a ciphertext that anyone of them could not decrypt on their own, independent randomization of secret keys of users is required.

2 RELATED WORK

In a CP-ABE, secret key of data user is represented by a trait set, and ciphertext is linked with the access policy structure defined only over the universe of trait set. The Key Authority could reverse the entire data users ciphertext to obtain the actual data, knowing the secret key of the data user, which no data user wants to reveal. The present CP-ABE technique do not support arbitrary state attributes and weighted attributes. In this paper, we have re-

visited the attribute-based data sharing technique which not only removes key escrow problem but also increases the expressiveness of the attribute, thus making the technique increasingly useful for cloud computing. We have proposed a better technique of two-party key issuing protocol which ensures that both Cloud service provider and Key authority cannot know the entire secret key of an individual user. Also, we have introduced the technique of weighted attribute, so that there is not only increase in the expressive power of an attribute, from binary to arbitrary state, but also there is simplification of the access policy. Hence, the cost of storage and complexity of encryption of a cipher text are reduced.

3 IMPLEMENTATION

The proposed system consists of a space of users with each user space having descriptive attributes. A set of users holding the attribute denotes an attribute group and this group is used as a user access. There may be many such attribute groups. The Key generation centre and the Data-storing center take part in protocol for issue of user key. Thus, in this protocol, a user has to request both the parties to acquire a set of keys. The Key generation centre authenticates a user eligible to the attributes and issues attribute keys to them. The generation of secret key occurs from the secure 2PC protocol of the Key generation centre and the Data-storage center as shown in Fig. 1. These two authorities take part in the secure 2PC protocol and they have their own master secret keys and these are issued as independent components of key to a user. Thus, the user generates the whole secret keys from independent key components issued by the two authorities. The secure 2PC protocol prevents the two authorities from knowing master secrets keys of each other and hence each of them alone will not be able to generate the whole secret keys of a user.

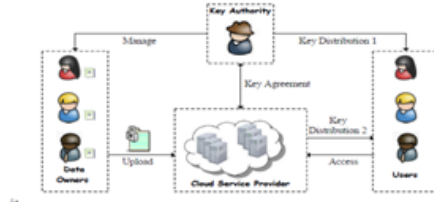


Fig.1 Proposed Architecture

The scheme of construction will contain the following stages.

- i System setup
- ii Data Encryption
- iii Key Generation
- iv Data Decryption

Stage 1: System setup: This phase includes two steps: KA:Setup and CSP:Setup.

- i. $KA_Setup(1k) \rightarrow (PP1, MSK1)$: In this process security parameter k is given as input and outputs a public parameter $PP1$ and a master secret key $MSK1$.
- ii. $CSP_Setup(1k) \rightarrow (PP2, MSK2)$: In this process security parameter k is given as input and outputs a public parameter $PP2$ and $MSK2$.

Here, $PP = PP1, PP2$ and $MSK = MSK1, MSK2$ are represented as public parameter and master secret key of system, where $MSK1$ and $MSK2$ are held by KA and CSP, respectively.

Stage 2: Data Encryption: In this symmetric encryption algorithm is used to enhance efficiency of encryption in which DO encrypts file M using content key ck , where file ciphertext is designated as $Eck(M)$. Then, the content key ck is encrypted by the following process.

$DO_Encrypt(PP, ck, A) \rightarrow (CT)$: PP , ck , and an access policy A are given as input by DO to the Encryption algorithm to encrypt ck and produces content key ciphertext CT as output which includes A . Then, DO provides $Eck(M)$ and CT to CSP.

Stage 3: User Key Generation: This stage consists of KA_KeyGen and CSP_KeyGen .

i. $KA_KeyGen(MSK1, S) \rightarrow (SK1)$: KA inputs MSK1 and a group of weighted attributes S which produces secret key SK1 represented by S. ii. In CSP_KeyGen , an improved 2PC protocol is proposed to remove key escrow issue. KA and CSP perform the 2PC protocol with their own master secret keys.

Therefore, neither KA nor CSP could produce the complete set of secret keys of end users alone.

$CSP_KeyGen(MSK2) \rightarrow (SK2)$: CSP KeyGen inputs MSK2 and the required information to produce secret key SK2 by accomplishing the key issuing protocol as shown below.

★ $KeyComKACSP(MSK1, IDt, MSK2)(SK2)$:

It is an interactive algorithm between KA and CSP. KA enters MSK1, and user identity IDt. CSP enters MSK2 and IDt. At last, only CSP generates a secret key component SK2 for the particular user. Then, the complete secret key SK is generated by the user from key components received independently from KA and CSP, where $SK = SK1, SK2$.

Stage 4: Data Decryption: This stage includes both algorithms: Users Decrypt and Data Decrypt. Firstly, cipher text file $Eck(M)$ and content key cipher text CT are downloaded from CSP. If user complies with conditions imposed by access policy, then content key ck is obtained by invoking Users: Decrypt algorithm. Then, user with ck could decrypt file M by executing Data: Decrypt operation.

i. $Users_Decrypt(PP, SK, CT) \rightarrow (ck)$: PP, SK described by S, and CT which contains access policy A are inputted by the user. Once the access policy A matches the weighted attribute set S, the content key ck is issued.

ii. $Data_Decrypt(Eck(M), ck) \rightarrow (M)$: $Eck(M)$ and ck are fed into symmetric decryption algorithm as input by the user and the file M is outputted.

We also introduced weighted attribute to improve expression from binary to arbitrary state which helps in simplification of access policy. This reduces the cost of storage and complexity of encryption of a ciphertext. For example, in a college Structure there are instructors consisting of Tutor, Assistant professor, Associate professor and Professor[7]. The weight of the attribute for each type of instructor is distributed as 1, 2, 3, and 4 and thus, these attributes can be termed as "Instructor: 1", "Instructor: 2", "

Instructor: 3" and "Instructor: 4", respectively. Thus, here one attribute has different weights, showing, arbitrary state attributes such as "Instructor: Tutor, Assistant Professor, Associate Professor and Professor". Here an access policy is denoted as: T ("Assistant Professor" OR "Associate Professor" OR "Professor") AND "Male", and the present CP-ABE technique is in the form of access policy T. If the proposed technique is used, the T can be simplified as T "Instructor: 2" AND "Male", since the attribute "Instructor: 2" indicates the minimum level in the access policy and includes "Instructor: 2", "Instructor: 3" "Instructor: 4". Thus, the storage and encryption cost of the cipher text can be reduced. These two structures are shown in Fig.2



Fig.2 T signifies existing CP-ABE technique. T' is proposed technique.

This proposed weighted CP-ABE technique can be used to express more attribute space than under the existing CP-ABE technique. Thus, if the attribute space and weighted set has n elements, the proposed system can have n^2 different possibilities whereas, the existing CPABE technique have $2n$ possibilities only.

4 CONCLUSION

In this paper, attribute-based data sharing technique in cloud computing has been redesigned with improvement of key issuing protocol to solve the key escrow problem. This increases confidentiality and privacy of the data in Cloud computing against the Key Authority and Cloud Service Provider as well as outsiders. Also, the weighted attribute is proposed to enhance the Attribute expression from binary to arbitrary state and this also simplifies the access policy and the cost of storage and encryption of cipher text are reduced.

References

- [1] M. Pirretti, P. Traynor, P. McDaniel, and B. Waters. Secure attribute-based systems. In Proceedings of the 13th ACM conference on Computer and communications security, pages 99112. ACM Press NewYork, NY, USA, 2006
- [2] A. Sahai and B. Waters, Fuzzy identity-based encryption, in Advance in CryptologyEUROCRYPT 2005. Springer, 2005, pp. 457473
- [3] Vipul Goyal, Omkant Pandey, Amit Sahai and Brent Waters, Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data ACM CCS (2006)
- [4] Bethencourt, J.; Sahai, A.; Waters, B. (2007-05-01). "Ciphertext-Policy Attribute-Based Encryption". 2007 IEEE Symposium on Security and Privacy (SP '07): 321334. doi:10.1109/SP.2007.11.
- [5] A. Shamir, How to share a secret, Communications of the ACM, vol. 22, no. 11, pp. 612613, 1979.
- [6] Identity-based cryptosystems and signature schemes, in Advances in cryptology. Springer, 1985, pp. 4753.
- [7] Shulan Wang, Kaitai Liang, Joseph K. Liu, JianyongChen, Jianping Yu, WeixinXie , "Attribute-Based Data Sharing Scheme Revisited in Cloud Computing", IEEE Transactions on Information Forensics and Security, 2016.

Guide Details

Mr. N.Vijaykumar was born in India. He received B.Tech degree in the year of 2005. & M.Tech PG in the year of 2011 from VIST, Bhongir. He was expert in Automata and Compilers Subjects. He is currently working as An Assistant Professor in the CSE Department in SR Engineering College, Hasanparthy, Warangal, Telangana State, India.

Student Details

Mr. T. SHASHANK was born in India. He is pursuing M.Tech degree in Computer Science & Engineering in CSE Department in

SR Engineering College, Hasanparthy, Warangal, Telangana State,
India.

