The Research on Multi-Authority Based Weighted Attribute Encryption Algorithm in the Cloud Computing Environment

SHEN Rui[1, a], ZHU Xuejun [2,b]

[1,2] College of Information Technology and Mass Media, Hexi University, Zhangye 734000

[a]shenrui@126.com

Keywords: Multi-Authority; Attribute-Based Encryption; Cloud Computing; Weighted Attribute Encryption

Abstract. In the cloud right weight attribute encryption scheme based on multi-agency. Under existing cloud computing environment based on multi-agency access control scheme generally do not take into account the weights of the attributes that the status attributes are equal. But in real life, with the right to property values are meaningful. Each attribute in the system that served as different roles, their respective importance in the system has also different. This paper presents a cloud right environment based on the weight attribute encryption scheme multi-agency, the introduction of property in the system weight concept, attribute authority based on the importance of the attributes assigned different weights, and based on the weight attributes, by attribute set segmentation algorithm set of attributes into the attribute weights stripe set, so the ciphertext and the weight threshold access structure associated, in order to achieve the right to re-attribute encryption scheme based on multi-agency. The program can reflect the importance of the property, making the program more practical significance.

Introduction

With the development of Internet and cloud computing in an open environment for data sharing and data processing needs more and more. Information technology to bring convenience, but also brought the security challenges [1-2]. Provider data when sharing data not only requires the flexibility to customize access control policies, but also to ensure the communication process between the data providers and users to ensure the confidentiality of data. In the cloud computing environment is an urgent need to support many communication mode, which reduces the huge overhead per user to encrypt the data brought.

Although existing broadcast encryption technology can solve some of the efficiency problems, but it is difficult to obtain the identity of the size and one-time member of the receiving group in the existing cloud computing environments. In order to meet flexible access control policy while ensuring the confidentiality of the data, literature [3] was first introduced property-based encryption (ABE) concept. The development of property-based encryption mechanism based on public key infrastructure (PKI) system based on the up, with a set of attributes that describe the user's identity, and the introduction of access structure to associate the user's secret Lang and ciphertext to attribute set and access structure, only when the user private key and the ciphertext match, users can decrypt it. It is because of this feature ABE, which can be removed from the ciphertext cost control access to key distribution occur frequently [4].

Although there are a lot of property-based encryption scheme, but these programs have a common characteristic, with little regard to the importance of the property, that is, the status attributes are equal. Since each attribute in the system that served as different roles, their respective systems has the voice is different. Thus, in real life, with the right to property values are meaningful [5-6]. Compared with the previous property-based encryption scheme, we will attribute weights introduced into the system, so that the program closer to the actual situation, and the reality of the system is meaningful. The program can be configured to support attribute weights while in the standard model can withstand indistinguishable chosen plaintext attack

The basic mechanism of Attribute-Based Encryption

The entities involved in the access control system of Attribute-Based Encryption (ABE)include the authority and users. Regulatory authority property and property keys issued to users: users into the message sender and recipient. Each attribute mapping system using a hash function to the Z, the ciphertext, and user keys are associated with the properties. The mechanism supports the policy thresholds based on attributes that only the user attributes set amount of the ciphertext attribute set to achieve the system elements intersect at a predetermined threshold parameter can decrypt [7]. ABE mechanisms include four kinds of basic algorithms: Setup, Extract, Encrypt, Decrypt. The runtime system initialization parameters according to security BDH parameter generator to produce two prime order q of the group G1, G2, and bilinear pairing e: G1 × G1 → G2. D stands for the threshold parameter.

KP-ABE mechanism shown in Figure 1, the user key to take the tree describe access policy A_{u-KP}, the leaf nodes of the tree collection is A_u. Ciphertext associated with a set of attributes A_c only A_c meet A_{u-KP}, the user can decrypt the ciphertext difference KP-ABE ABE and basic mechanisms in KeyGen and Decrypt algorithm.

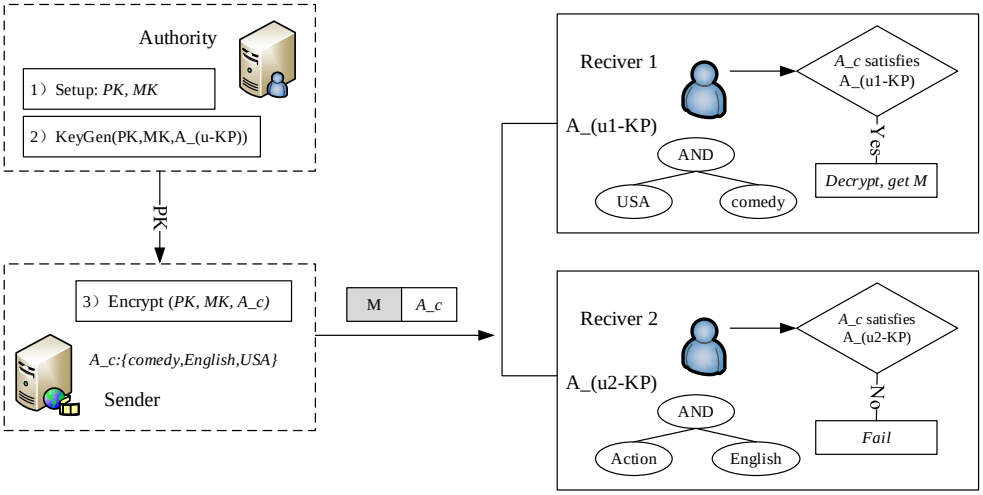

Figure 1. KP-ABE mechanism illustration

The current KP-ABE implement complex access structure to support flexible access policies. Based on the assumption DBDH achieve flexibility and CP-ABE CPA security in public policy making system design complexity limits the access structure design. ABE system towels, dynamic attributes increases the complexity of key revocation; and property keys and user identity has nothing to do, making it impossible to prevent and trace illegal users who have a legitimate user's private key (pirate key). The large-scale distributed applications that require multi-agency coordination mechanisms to support ABE. To meet malleability, fault tolerance needs to study these factors ABE's challenges.

ABE belong to a single authority basic situation, cannot meet the demand for large-scale distributed applications collaboration of different agencies; authority must be fully credible, contrary to the requirements of distributed applications trust the security needs of decentralized; authority management system for all properties, as Users issue key, heavy workload, becomes the system performance bottlenecks. ABE more authority not only to meet the needs of distributed applications, and can be trusted and workload single authority is dispersed to all the authority of the system, it is multi-institutional research ABE case is necessary. However, each authority issued an independent key and user key demand accuracy, to a multi-agency study of challenges ABE.

Key-policy weighted attribute based encryption scheme and security model

Cloud computing environment based on more authority attribute encryption scheme has important significance. Before many of these programs generally do not take into account the weights of the attributes, status hypothesis attributes are equal. But in real-world applications, the

property has the right value is meaningful. Each property in the system plays a different role, and accordingly they are in the system. Importance is also different. This article describes a cloud computing environment based on the right authority multi-agency re-attribute encryption scheme, compared with the multi-agency attribute encryption scheme before the next cloud computing environment, we have introduced important attribute in the system, making the program more practical significance.

In this section, we define the system model of our multi-authority based weighted attribute encryption scheme in cloud computing, and then define the security model. A multi-authority access control scheme is considered as described in Figure 2 [8]. Attribute encryption scheme more authority is more suitable for data access control cloud storage system, because the user can be held by multiple institutions to manage property, and access to policy data owner to use the property may be defined in different institutions. Traditional single authority to manage all user attributes dense steel, easy to degrade system performance. In addition, a single authority solution requires authorized body completely honest, it is difficult to meet the security requirements of cloud computing environments.

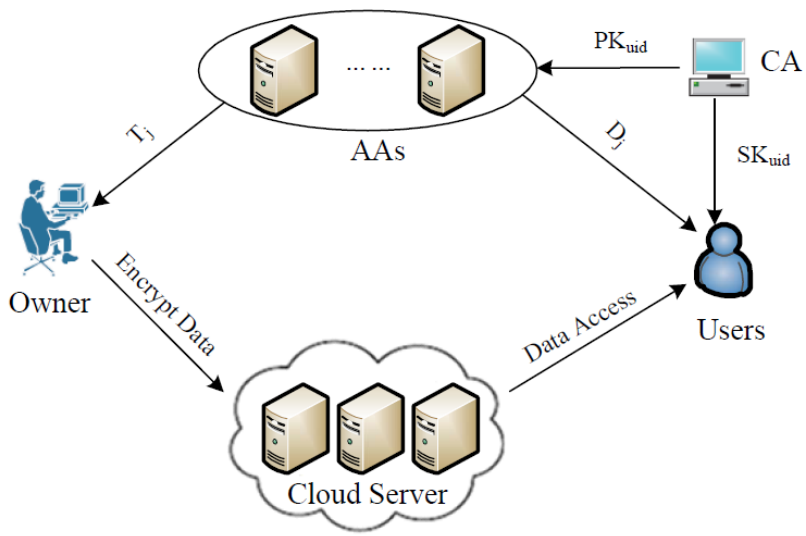

Figure 2. System model of multi-authority based access control scheme

There are five entities in the system: the data owner (Owner), the cloud server (Cloud Server), the multiple attribute authorities (AAs), a central authority (CA) and the data consumers (users). The owner defines the access control policy and encrypts its data under the policy before uploading it to the cloud server. The cloud server provides data storage service to the data owner and access service to users. Each AA is an independent entity that entitles, updates and revokes user's attributes in its administration domain. Every attribute is associated with an AA, but each AA manages any number of attributes. The CA is a trusted entity which is responsible for assigning a global user identifier *uid* for every user and the user's system public key PK_{uid} for AAs. However, the CA does not manage any attribute in the system and creates the user's secret keys that are associated with attributes.

We introduce key-policy weighted attribute based encryption (KP-WABE) scheme and its security model.

KP-WABE scheme

There are four fundamental algorithms consisted in KP-WABE scheme: Setup, KeyGen, Encrypt and Decrypt.

Setup (1^{λ}, U): The setup algorithm is run by central authority which inputs security parameter 1^{λ} and weighted attribute universe description U. It will generate the public parameters pms and master key MSK as output after the Setup algorithm run completely.

KeyGen (*pms*, *MSK*, Γ): The key generation algorithm is run by central authority which takes public parameters *pms*, master key *MSK* and weighted access structure Γ as input. It will generate a private key SK which contains Γ as output after executing the KeyGen algorithm.

Encrypt (*pms*, S'_o, *m*): This encryption algorithm is run by a user who wants to protect the message which takes the public parameters *pms*, the message m and a set $S'_o 0$ of weighted attributes *S* as input. It will generate a ciphertext CT as output after executing the Encrypt algorithm.

Decrypt (CT, SK): The decryption algorithm is run by decryptor which takes the ciphertext CT and the private key SK as input. If a set of weighted attribute satisfies the weighted access structure, it will generate the ciphertext and return message m as output after executing the Decrypt algorithm.

In the KP-WABE scheme, the ciphertext is related with a weighted attribute set while the private key is associated with the weighted access structure. In our security model, the adversary will choose a challenged access structure Γ^* and ask for any private key SK contain weighted attribute set S which does not satisfy Γ^*. We now give the formal security game for KP-WABE scheme below.

Security model for KP-WABE

Init. The adversary first declares a challenged weighted attribute set S which he wants to be challenged upon.

Setup. The challenger runs the Setup algorithm and outputs the public parameter pms. The pms will given to the adversary after executing Setup algorithm successfully.

Phase 1. In this phase, the adversary will make polynomially private key queries for many weighted access structures Γ_j repeatedly. It is worth noting that S is not satisfied any weighted access structure Γ_j.

Challenge. After finishing Phase 1, the adversary A will submits two equal length message $m_0, m_1 \in M$ to the challenger. Then, challenger flips a random coin β and encrypts $m_{\beta,}$ with S. After flipping the coin, the encrypted message is given to the adversary A.

Phase 2. Same as phase 1.

Guess. The adversary outputs a guess whether $\beta' = \beta$ or not.

If $\beta' = \beta$, we say the adversary A wins this game. We defined the advantage of A as $\mathbf{Adv}_A = \Pr[\beta' = \beta] - \frac{1}{2}$ in this game.

Conclusion and discussion

In order to achieve confidentiality of communication, the encryption is considered to be the most widely used mechanisms, in order to protect the transmission of messages. With the emergence in recent years many new applications, in order to protect the confidence of information, there are new challenges. As we come in the cloud computing era, many companies outsource their storage capacity to store personal information. However, the cloud server cannot be fully trusted transaction company. In addition, due to the characteristics of cloud computing, different users want to share their files to meet specific user group policies. Using conventional methods, conveniently while achieving both of these features, it is difficult. Recently, attribute-based encryption technology has become a new public key raw attracted a lot of attention. It has outstanding advantages over conventional PKC because it can achieve information security and granular access control based encryption attribute (ABE). When the data provider you want to use the traditional method to share some information with users, suppliers must know that he/she wishes to share with accurate information. Abe plans can easily solve this problem, many flexible encryption, rather than one to one. In this scenario, the encrypted text is marked as a set of attributes or access the system user-defined structure. A particular user's private key can decrypt the cipher text given only if the two match.

In this paper, we propose a program, known as the key policy-weighted attribute-based encryption (KP-WABE) program. In reality, the property is not always in the same position. Different properties have different importance in the system. Each data receiver has a set of weighted attribute. The data owner for all receivers should have a certain weight attributes will be encrypted. In KP-WABE program, some kind of weighted data access architecture of the recipient's private key. In order to effectively decrypt the message, encrypted text has a set of weighted attribute access structure must satisfy weighting.

References

[1] Liu X, Jianfeng M A, Xiong J, et al. Ciphertext-Policy Weighted Attribute Based Encryption Scheme[J]. Journal of Xian Jiaotong University, 2013, 47(8):44-43.

[2] Khader D. Introduction to Attribute Based Searchable Encryption[M]// Communications and Multimedia Security Springer Berlin Heidelberg, 2014:131-135.

[3] Sahai A, Waters B. Fuzzy Identity-Based Encryption[M]// Advances in Cryptology–EUROCRYPT 2005Springer Berlin Heidelberg, 2005:457-473.

[4] Liu X, Zhu H, Ma J, et al. Key-Policy Weighted Attribute based Encryption for fine-grained access control[C]// Communications Workshops (ICC), 2014 IEEE International Conference on IEEE, 2014:694-699.

[5] Wang Y, Zhang D, Zhong H. Multi-authority based weighted attribute encryption scheme in cloud computing[C]// Natural Computation (ICNC), 2014 10th International Conference on IEEE, 2014:1033-1038.

[6] Wang C, Cao N, Li J, et al. Secure ranked keyword search over encrypted cloud data[C]//Distributed Computing Systems (ICDCS), 2010 IEEE 30th International Conference on. IEEE, 2010: 253-262.

[7] Li R, Xu Z, Kang W, et al. Efficient multi-keyword ranked query over encrypted data in cloud computing[J]. Future Generation Computer Systems, 2014, 30: 179-190.

[8] Wang Y. Research on Access Control with attribute-based encryption in Cloud Computing. Anhui University (in Chinese).