Accessing Cloud as Public and Private with Privacy Schemes

B.SHRAVYA, M.MOUNIKA, K.VARUN RAJ, VINEETH KUMAR
Under guidance of M.AGNISHA
B. Tech Department of Computer Science and Engineering
St. Martin's Engineering College, Hyderabad, Telangana, India

ABSTRACT

With the rapid development of the computer technology, cloud-based services have become a hot topic. Cloud based services not only provide users with convenience, but also bring many security issues. Therefore, the study of access control scheme to protect users' privacy in cloud environment is of great significance. In this paper, we present an access control system with privilege separation based on privacy protection (PS-ACS). In the PS-ACS scheme, we divide the users into personal domain (PSD) and public domain (PUD) logically. In the PSD, we set read and write access permissions for users respectively. The Key-Aggregate Encryption (KAE) is exploited to implement the read access permission which improves the access efficiency. A high degree of patient privacy is guaranteed simultaneously by exploiting an Improved Attribute-based Signature (IABS) which can determine the users' write access. For the users of PUD, a hierarchical attribute-based encryption (HABE) is applied to avoid the issues of single point of failure and complicated key distribution. Function and performance testing result shows that the PS-ACS scheme can achieve privacy protection in cloud based services.

1. INTRODUCTION

Data security issues brought by data sharing have seriously hindered the development of cloud computing, various solutions to achieve encryption and decryption of data sharing have been proposed. In this paper, we present an access control system with privilege separation based on privacy protection (PS-ACS). In the PS-ACS scheme, we divide the users into personal domain (PSD) and public domain (PUD) logically. In the PSD, we set read and write access permissions for users respectively. The Key-Aggregate Encryption (KAE) is exploited to implement the read access permission which improves the access efficiency. A high degree of patient privacy is guaranteed simultaneously by exploiting an Improved Attribute-based Signature (IABS) which can determine the users' write access. For the users of PUD, a hierarchical attribute-based encryption (HABE) is applied to avoid the issues of single point of failure and complicated key distribution. Function and performance testing result shows that the PS-ACS scheme can achieve privacy protection in cloud based services.

2. LITERATURE SURVEY

Dynamic and Efficient Key Management for Access Hierarchies

In this defined a key allocation mechanism that implements such an access graph, that is, an assignment of keys to users and objects where a user can access an object if he has a key for that object.

The paper concludes with the number of keys increases with the number of branches. It is unlikely to come up with a hierarchy that can save the number of total keys to be granted.

Patient Controlled Encryption: Ensuring Privacy of Electronic Medical Records[3]

In this paper build an efficient system that allows patients both to share partial access rights with others, and to perform searches over their records.

The paper concludes with the encryptor needs to get the secret keys to encrypt data which is not suitable for many applications. It is unclear how to apply this method for public key encryption scheme.

Practical LeakageResilient IdentityBased Encryption from Simple Assumptions[4]

Identity-based encryption (IBE) is a type of public-key encryption in which the public-key of a user can be set as an identity-string of the user (e.g., an email address)

The paper concludes with the different secret keys have to be generated for the same identities, and as a result it is more difficult to apply leakage resilient techniques.

Improving Privacy and Security in Multi-Authority Attribute-Based Encryption[5]

In this scheme multiple attribute authorities monitor different sets of attributes and issue corresponding decryption keys to user and encryptors can require that a user obtain keys for appropriate attributes from each authority before decrypting a message

The paper concludes with the size of the key often increases with the number of attributes it encompasses or the ciphertext-size is not constant.

3. OVERVIEW OF THE SYSTEM

ARCHITECHTURE

Sentiment analysis is the most important task in extracting user's interest preferences. The sentiment is used to find customer's personal review on the product.Before that, there are directly star rating options available by which user select number of stars on its own experience of the product, but not all website have star rating factor.To make a more accurate rating user sentiment takes an important role. Reviews are in two types positive or negative.

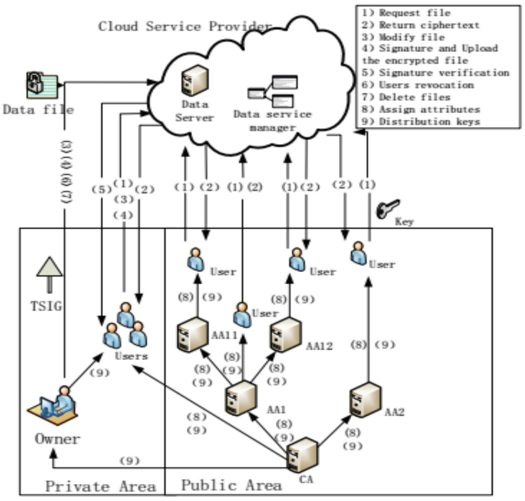

Fig 3.1 Architecture of accessing cloud

As shown in Fig.1, our system model consists of Data owner, users in PSD, and users in PUD, root authority CA, regional authority AA and cloud service provider, which are defined as follows.

1. The cloud service provider consists of two parts: data storage server and data service management. Data storage server is responsible for storing confidential data files, and data service management is in charge of controlling external users' access to secret data and returning the corresponding cipher text.

2. In the actual cloud environment, CA manages multiple AA, and AA each manages attributes in their own field. The attributes owned by the user are issued by different authority.

3. Personal domain (PSD), in which users have special privileges, such as family, personal assistant, close friends and partners. This domain has a small number of users and small scale attributes, and the data owner knows the user's identity, which is easy to manage.

4. Public domain (PUD), which owns a huge number of users with unknown identity and a lot of attributes owned by the user.

5. Data Owner based on the characteristics of users in public and personal domain to develop different access control strategy, encrypt uploaded files using the corresponding encryption method and then sends to the cloud server.

4. MODULES

It consists of four modules. They are:

- Data owner Module
- Personal Domain (PSD) Module
- Public Domain (PUD) Module
- Cloud Service Provider Module

Data owner module:

Data Owner, based on the characteristics of users in public and personal domain to develop different access control strategy, encrypt uploaded files using the corresponding encryption method and then send to the cloud server.

Personal domain module:

Personal domain (PSD) in this user has special privileges, such as family, personal assistant, close friends and partners. This domain has a small number of users and small scale attributes, and the data owner knows the user's identity, which is easy to manage.

Public domain module:

Public domain (PUD), it owns a huge number of users with unknown identity and a lot of attributes owned by the user.

Cloud service provider:

The cloud service provider consists of two parts: data storage server and data service management. Data storage server is responsible for storing confidential data files, and data service management is in charge of controlling external users' access to secret data and returning the corresponding cipher text.

5. ALGORITHM

ACCESS CONTROL SCHEME IN PSD

Read Access Control

The PSD has a small number of users, and their identities are known to the owner. In general, the data owner only wants the users to access or modify parts of data files, and different users can access and modify different parts of the data. This requires the data owner to grant users read or write access permission to some data. In Chen's MAH-ABE scheme, the CP-ABE is used to achieve the read access permission, but there are some defects to be considered. Firstly, since in the PSD, the users are all have a close relationship with the owner and the number is small, there is no need to use the CP-ABE which is applicable to the scenario which has a lot of users, and their identities are unknown to the owner, while the KAE scheme is set for the small users with certain identities. Besides, the distribution and management of keys and attributes, encryption and decryption process of CP-ABE are much more complex compared with the KAE scheme. Therefore, the KAE is exploited to implement the read access permission which improves the access efficiency. Based on the above analysis, the paper uses the Aggregate Key Encryption scheme to encrypt the data files to realize different read access control. The specific application process of the KAE algorithm is as follows.

1. System setup and file encryption:

The system first runs Setup of KAE to establish the public system parameter and master key. Then the owner's client application runs Encrypt of KAE using the public key and the number of classification file to encrypt the PHR files and sends them to the cloud.

2. Access and key distribution:

When the user send access request to the cloud server, and his file index number is i, then the cloud server returns the corresponding encrypted classification file to the user. The owner authorized users access permission with the file index number denoted by j and sent the collection S of all the index number j to CA, CA generate an aggregate decryption key for a set of cipher text classes via Extract of KAE and sent it to the corresponding user, Finally, any user with an aggregate key can decrypt any cipher text whose class is contained in the aggregate key via Decrypt of KAE.

Write Access Control

As Chen's MAH-ABE scheme does not refer to the write access control, and in the PSD some cases exist, for example, the owner needs his friends to modify his file after he read it. So we proposed the write access permission in the PSD. For the user, the public key and file class label are all known, he can implement the algorithm to encrypt the files after he modified, and then upload them to the cloud. But whether the cloud server saves the modified file is decided by the write access control policy. On the one hand, in the complex cloud environment, if a user's modification operations are very frequent, maybe he is very important to the user, so that the user may be stricken from outside attacks. Therefore, the user worries the leak of identity after the signature. On the other hand, in the data sharing scheme, the separate access of read and write to the file is extremely important. In PSD, not all users who have read permissions also have write permissions to the files. Whether the user has write permissions to the file is decided by the data owner. Therefore, this paper selects the improved attribute-based signature (IABS) to determine the user's write permission. The main structure of the scheme includes five parts: an authentication center (CA), the data owner, users, mediator and cloud servers. The CA is responsible for generating master key which is sent to the owner and system parameters which are shared for all users. The mediator holds part components of the signature keys and is responsible for the validity check of attributes and users. The data owner produces the signature tree and sends it directly to the cloud server. The user encrypts the modified files and signs them using the attribute-based signature, then uploads them to the cloud server. The cloud server verifies the attribute-based signature, if the authentication is successful, the user has permission to modify files and the cloud server stores the file. Own to the limited space we will omit the specific description of the IABS scheme in PSD.

ACCESS CONTROLSCHEME IN PUD

The PUD is characterized by a huge number of users, a lot of attributes owned by the user, complexity management, and indefinite users' identity. In view of the above characteristics, the user can only have the read access permission. Although the attribute-based encryption scheme (CP-ABE) can achieve access control, it cannot meet the needs of complex cloud environment. In traditional CP-ABE scheme, there is only one authorized agency responsible for the management of attributes and distribution of keys. The data owner defines access policies and encrypts the data files in accordance with this policy. Each user is distributed a key related to his attribute. As long as the user's attributes meet the access policy he can decrypt the file. However, if there is only one authority in the system and all public and private keys are issued by the authority. Two problems will appear in the practical application:

1. In the practical cloud environment, there are a lot of authorities and each authority in their own field manages part of users' attributes. The attributes owned by the user are issued from different authorities

2. If there is only one authority, all the distribution of the keys are handed over by one trusted authority. The frequent interaction between the user and trust authority will not only bring bottlenecks for the system load capacity, but also increase the potential security risks. Therefore, multi authority ABE (MA-ABE) is used in this paper. Users in PUD do not need to interact directly with the data owner, and the attributes of the user are called role attributes. Firstly the data owner uploads the attribute-based encrypted data files to the cloud server. Then after authorized, the data owner receives the corresponding decryption key and sends a data file access request directly from the cloud server. Finally, after the cloud server returns the cipher text, users can use their own decryption key to decrypt the cipher text.

B. Access Control Process Based on the above analysis, we use a hierarchical attribute encryption scheme (HABE) to implement access control in PUD.

6. CONCLUSION

In this paper, we propose access control system (PS-ACS), which is privilege separation based on privacy protection. Through the analysis of cloud environment and the characteristics of the user, we divide the users into personal domain (PSD) and public domain(PUD) logically. In the PSD, the KAE algorithm is applied to implement users read access permissions and greatly improved efficiency. The IABS scheme is employed to achieve the write permissions and the separation of read and write permissions to protect the privacy of the user's identity. In the PUD, we use the HABE scheme to avoid the issues of single point of failure and to achieve data sharing. Furthermore, the paper analyzes the scheme from security and efficiency, and the simulation results are given. By comparing with the MAH-ABE scheme, the proposed scheme shows the feasibility and superiority to protect the privacy of data in cloud-based services.

7. REFERENCES

[1] S. Yu, C. Wang, K. Ren, "Achieving secure, scalable, and fine-grained data access control in cloud computing," Proc. IEEE INFOCOM, pp. 1-9, 2010.

[2] J. Bethencourt, A. Sahai, B. Waters, "Ciphertext-policy attribute-based encryption," Proc. Security and Privacy, pp. 321-334, 2007.

[3] J. Hur, D.K. Noh, "Attribute-based access control with efficient revocation in data outsourcing systems," IEEE Transactions on Parallel and Distributed Systems, vol. 22, no. 7 pp. 1214-1221, 2011.

[4] A. Lewko, B. Waters, "Decentralizing attribute-Based encryption," Proc. Advances in Cryptology-EUROCRYPT, pp. 568-588, 2011.

[5] M. Li, S. Yu, Y. Zheng, "Scalable and secure sharing of personal health records in cloud computing using attribute-Based Encryption," IEEE Transactions on Parallel and Distributed System, vol. 24, no. 1, pp. 131143, 2013. [6] C.K. Chu, S.S.M. Chow, W.G. Tzeng, "Key-aggregate cryptosystem for scalable data sharing in cloud storage," IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 2, pp.468-477, 2014. [7] J. Li, K. Kim, "Hidden attribute-based signatures without anonymity revocation," Information Sciences, vol. 180, no. 9, pp. 1681-1689, 2010.

[8] H.K. Maji, M. Prabhakaran, M. Rosulek, "Attribute-Based Signatures," Proc. Topics in Cryptology - CT-RSA, pp. 376-392, 2011.

[9] S. Kumar, S. Agrawal, S. Balaraman, "Attribute based signatures for bounded multi-level threshold circuits," Proc. Public Key Infrastructures, Services and Applications, pp. 141-154, 2011.