© 2018 IJSRST | Volume 4 | Issue 7 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X
Themed Section: Science and Technology

A Novel Approach Secure Data Sharing for Mobile Cloud Computing

B. Sushmitha[1], K. Sree Harsha[2], N. Srilatha[2], T. Sneha[2]
[1]Assistant Professor, Department of Information Technology in Teegala Krisha Reddy Engineering College,Telangana, India
[2]UG Scholar, Department of Information Technology in Teegala Krisha Reddy Engineering college, Telangana, India

ABSTRACT

With the popularity of cloud computing, mobile devices can store/retrieve personal data from anywhere at any time. Consequently, the data security problem in mobile cloud becomes more and more severe and prevents further development of mobile cloud. There are substantial studies that have been conducted to improve the cloud security. However, most of them are not applicable for mobile cloud since mobile devices only have limited computing resources and power. Solutions with low computational overhead are in great need for mobile cloud applications. In this paper we propose an access control technology used in normal cloud environment, but changes the structure of access control tree to make it suitable for mobile cloud environments.

Keywords : Mobile Cloud Computing, Data Encryption, Access Control, User Revocation

I. INTRODUCTION

Nowadays, various cloud mobile applications have been widely used. In these applications, people (data owners) can upload their photos, videos, documents and other files to the cloud and share these data with other people (data users) they like to share. CLOUD SERVICE PROVIDERs also provide data management functionality for data owners. Since personal data files are sensitive, data owners are allowed to choose whether to make their data files public or can only be shared with specific data users. Clearly, data privacy of the personal sensitive data is a big concern for many data owners.

The state-of-the-art privilege management/access control mechanisms provided by the CLOUD SERVICE PROVIDER are either not sufficient or not very convenient. They cannot meet all the requirements of data owners. First, when people upload their data files onto the cloud, they are leaving the data in a place where is out of their control, and the CLOUD SERVICE PROVIDER may spy on user data for its commercial interests and/or other reasons. Second, people have to send password to each data user if they only want to share the encrypted data with certain users, which is very cumbersome. To simplify the privilege management, the data owner can divide data users into different groups and send password to the groups which they want to share the data. However, this approach requires fine-grained access control. In both cases, password management is a big issue.

Apparently, to solve the above problems, personal sensitive data should be encrypted before uploaded onto the cloud so that the data is secure against the CLOUD SERVICE PROVIDER. However, the data encryption brings new problems. How to provide efficient access control mechanism on ciphertext decryption so that only the authorized users can access the plaintext data is challenging. In addition, system must offer data owners effective user privilege management capability, so they can grant/revoke data access privileges easily on the data users. There have

been substantial researches on the issue of data access control over ciphertext. In these researches, they have the following common assumptions. First, the CLOUD SERVICE PROVIDER is considered honest and curious. Second, all the sensitive data are encrypted before uploaded to the Cloud. Third, user authorization on certain data is achieved through encryption/decryption key distribution. In general, we can divide these approaches into four categories: simple ciphertext access control, hierarchical access control, access control based on fully homomorphic encryption and access control based on data set.All these proposals are designed for non-mobile cloud environment. They consume large amount of storage and computation resources, which are not available for mobile devices. According to the experimental results in each data, the basic data operations take much longer time on mobile devices than laptop or desktop computers. It is at least 27 times longer to execute on a smart phone than a personal computer computer. This means that an encryption operation which takes one minute on a PC will take about half an hour to finish on a mobile device. Furthermore, current solutions don't solve the user privilege change problem very well. Such an operation could result in very high revocation cost. This is not applicable for mobile devices as well. Clearly, there is no proper solution which can effectively solve the secure data sharing problem in mobile cloud. As the mobile cloud becomes more and more popular, providing an efficient secure data sharing mechanism in mobile cloud is in urgent need.

II. OBJECTIVE

The data confidentiality is taken into account from two aspects. In security, data are encrypted with a symmetric key. The security of this part is guaranteed by symmetric encryption mechanism. Next, the symmetric key is encrypted by attribute encryption. The security of this part depends on the encryption process. The security of the core algorithm in the encryption process is proved in the previous section. Here, we discuss the situation that the symmetric key is safe even if a malicious user, The conspiracy attack can be divided into several kinds, namely conspiracy between different users.consider the conspiracy between different users. It can be proven that different users with different attributes cannot combine their attributes to decrypt data files. Since users get different r from TA, which is used to generate attribute keys for users, different users with same attributes get different keys. When decrypting data files, only when all the keys are generated from the same r can they be combined to decrypt data files, thus effectively preventing the conspiracy between users. Second, consider the conspiracy between users.\

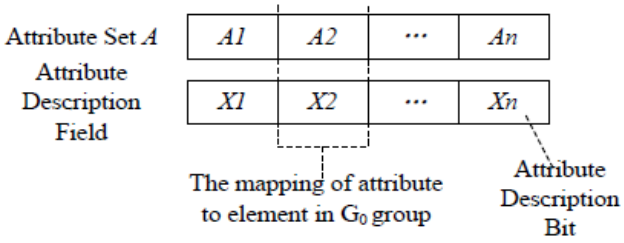

Figure 1: Data description general method

The process of user authorization executes to generate attribute keys for data users. The specific process is described as follows.

(1)logins onto the system and sends, an authorization request to third party. The authorization request includes attribute keys which data unit already has.

(2) third party authority accepts the authorization request and checks whether data unit has logged on before. If the user hasn't logged on before, go to step (3) , otherwise go to step (4).

(3) third party authority calls every authority function to generate attribute keys private key for data unit.

(4) Third part authority compares the attribute description field in the attribute key with the attribute description field stored in database. If they are not match, go to step (5),

(5) For each inconsistent bit in description field, if it is 1 on data user's side and 0 on third part authority side,

it indicates that data unit attribute has been revoked, then third party authority does nothing on this bit. If it is reversed scenario, it indicates that data unit has been assigned with a new attribute, then third party authority generates the private key.

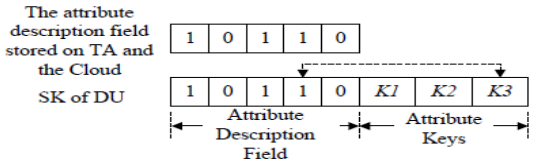

Figure 2 : data description of user

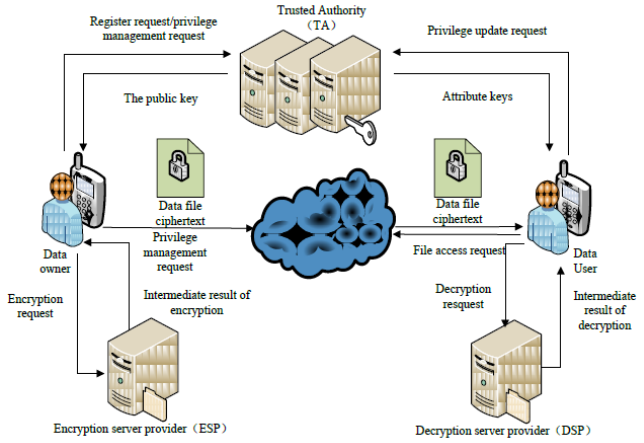

Figure 3 : data flow with serurity considerations

III. PROPOSAL

In summary, current proposals on data access control in the cloud are mostly for non-mobile terminals, which is not suitable for mobile devices. Besides, current solutions don't solve the problem of user privilege change scenarios very well since they bring high revocation cost. This is not applicable for mobile devices which only have limited computing capacity and power. Existing studies on mobile cloud don't have a good solution to secure data sharing when servers are not credible. In a word, there is no proper solution that can solve the problem of secure data sharing in mobile cloud. In a word, there is no proper solution that can solve the problem of secure data sharing in mobile cloud. a technology used in access control in the normal cloud environment, but changes the structure of access control tree to make it suitable for mobile cloud.

Hierarchical access control has good performance in reducing the overhead of key distribution in ciphertext access control. As a result, there are substantial research on ciphertext access control based on hierarchical access control method. In hierarchical access control method, keys can be derived from private keys and a public token table. However, the operation on token table is complicated and generates high cost. Besides, the token table is stored in the cloud. Its privacy and security cannot be guaranteed. Access control is an important mechanism of data privacy protection to ensure that data can only be acquired by legitimate users. There has been substantial research on the issues of data access control in the cloud, mostly focusing on access control over cipher text. Typically, the cloud is considered honest and curious. Sensitive data has to be encrypted before sending to the cloud. User authorization is achieved through key distribution.

IV. CONCLUSIONS

In recent years, many studies on access control in cloud are based on environment. However, traditional access is not suitable for mobile cloud because it is computationally intensive and mobile devices only have limited resources. in mobile cloud and reduce the overhead on users' side in mobile cloud. In the future work, we will design new approaches to ensure data integrity. To further tap the potential of mobile cloud, we will also study how to do ciphertext retrieval over existing data sharing schemes.

V. REFERENCES

[1]. Gentry C, Halevi S. Implementing gentry's fully-homomorphic encryption scheme. in: Advances in Cryptology–EUROCRYPT 2011. Berlin, Heidelberg: Springer press, pp. 129-148, 2011.

[2]. Brakerski Z, Vaikuntanathan V. Efficient fully homomorphic encryption from (standard) LWE. in: Proceeding of IEEE Symposium on Foundations of Computer Science. California, USA: IEEE press, pp. 97-106, Oct. 2011.

[3]. Qihua Wang, Hongxia Jin. "Data leakage mitigation for discertionary access control in collaboration clouds". the 16th ACM Symposium on Access Control Models and Technologies (SACMAT), pp.103-122, Jun. 2011.

[4]. Adam Skillen and Mohammad Mannan. On Implementing Deniable Storage Encryption for Mobile Devices. the 20th Annual Network and Distributed System Security Symposium (NDSS), Feb. 2013.

[5]. Wang W, Li Z, Owens R, et al. Secure and efficient access to outsourced data. in: Proceedings of the 2009 ACM workshop on Cloud computing security. Chicago, USA: ACM pp. 55-66, 2009.

[6]. Maheshwari U, Vingralek R, Shapiro W. How to build a trusted database system on untrusted storage. in: Proceedings of the 4th conference on Symposium on Operating System Design & Implementation-Volume 4. USENIX Association, pp. 10-12, 2000.

[7]. Kan Yang, Xiaohua Jia, Kui Ren: Attribute-based fine-grained access control with efficient revocation in cloud storage systems. ASIACCS 2013, pp. 523-528, 2013.

[8]. Crampton J, Martin K, Wild P. On key assignment for hierarchical access control. in: Computer Security Foundations Workshop. IEEE press, pp. 14-111, 2006.

[9]. Shi E, Bethencourt J, Chan T H H, et al. Multi-dimensional range query over encrypted data. in: Proceedings of Symposium on Security and Privacy (SP), IEEE press, 2007. 350-364

[10]. Cong Wang, Kui Ren, Shucheng Yu, and Karthik Mahendra Raje Urs. Achieving Usable and Privacy-assured Similarity Search over Outsourced Cloud Da ta. IEEE INFOCOM 2012, Orlando, Florida, March 25-30, 2012

[11]. Yu S., Wang C., Ren K., Lou W. Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing. INFOCOM 2010, pp. 534-542, 2010 .

[12]. Kan Yang, Xiaohua Jia, Kui Ren, Bo Zhang, Ruitao Xie: DAC-MACS: Effective Data Access Control for Multiauthority Cloud Storage Systems. IEEE Transactions on Information Forensics and Security, Vol. 8, No. 11, pp.1790-1801, 2013.