ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

A Less Weight Secure Data Sharing Scheme for Mobile Cloud Computing

P. Likitha
Department of Computer Science and Engineering,
MJR College of Engineering & Technology,
Piler, A.P - 517214, India.

Karamala Suresh
Department of Computer Science and Engineering,
MJR College of Engineering & Technology,
Piler, A.P - 517214, India.

ABSTRACT:

Mobile cloud computing is gaining popularity among mobile users. 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. The main challenge faced by everyone is to share the data all over the world or at organizational level securely without giving away the important data to any exploiters. To overcome this challenge to share the data securely through cloud, an efficient data encryption algorithm for encrypting data before sending it to the cloud. In this paper, we propose a lightweight data sharing scheme (LDSS) for mobile cloud computing. It adopts CP-ABE, 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. LDSS moves a large portion of the computational intensive access control tree transformation in CP-ABE from mobile devices to external proxy servers. Furthermore, to reduce the user revocation cost, it introduces attribute description fields to implement lazy-revocation, which is a thorny issue in program based CP-ABE systems. The experimental results show that LDSS can effectively reduce the overhead on the mobile device side when users are sharing data in mobile cloud environments.

***Keywords:* mobile cloud computing, data encryption, access control, user revocation.**

I. INTRODUCTION

Cloud computing means storing the data and accessing the data through the internet instead of using traditional hardware for most of the operations. More than 50% of IT companies have moved their Business to the cloud. With the development of cloud computing and the popularity of smart mobile devices, people are gradually getting accustomed to a new era of data sharing model in which the data is stored on the cloud and the mobile devices are used to store/retrieve the data from the cloud. Typically, mobile devices only have limited storage space and computing power. On the contrary, the cloud has enormous amount of resources. In such a scenario, to achieve the satisfactory performance, it is important to use the resources provided by the cloud service provider (CSP) to store and share the data. When any of the people upload the data onto the cloud they are leaving their data in a place where monitoring over that data is out of their control, the cloud service provider can also spy on the personal data of the users. When someone has to share data through the data they have to share the password to each and every user for accessing the encrypted data which is cumbersome. Therefore, to solve this problem data should be encrypted before uploading it onto the cloud which can be safe from everyone.

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. CSPs also provide data management functionality for data holders. Since personal data files are sensitive, data holders are allowed to choose whether to make their data files public or can

Cite this article as: P. Likitha & Karamala Suresh, "A Less Weight Secure Data Sharing Scheme for Mobile Cloud Computing", International Journal & Magazine of Engineering, Technology, Management and Research, Volume 5 Issue 7, 2018, Page 51-55.

only be shared with specific data customers. Clearly, data privacy of the personal sensitive data is a big concern for many data holders. Apparently, to solve the above issue, personal sensitive data should be encrypted before uploaded onto the cloud so that the information is secure across the CSP. However, the data encryption brings new issues. How to provide efficient access control mechanism on cipher text decryption so that only the authorized persons can access the plaintext data is challenging. In addition, system must offer data holder's effective user privilege management capability, so they can grant/revoke information access privileges easily on the data users. Now the data encryption part brings some new issues such as we have to provide an efficient encryption algorithm such that if the data is in encrypted format it cannot be easily to get break or get accessed by any exploiters. The next big concern is time consumption for encryption. Traditional Hardware with big configuration can encrypt data in short amount of time but limited resource devices suffer from this issue. They require more amount of time of encryption and decryption. So, an efficient crypto system is to be proposed which can worked equally or heterogeneously on all of the devices.

II. EXISTING SYSTEM

Attribute-based encryption (ABE) is proposed by Sahai and Waters. Attribute-based encryption (ABE) is a moderately late approach that re-evaluates the idea of public key cryptography. Attribute-based encryption is also referred to as ABE is a sort of public-key encryption wherein the secret key of a person and the cipher-text is established upon attributes. In an ABE, a person's keys and cipher-texts are labelled with units of descriptive attributes and a symmetric key can decrypt a selected cipher-text only if there's a match between the attributes of the cipher-text and the person's key. It reduces the quantity of key used and hence makes encryption and decryption technique faster. There have been substantial researches on the issue of information access control over cipher text. In these researches, they have the following common assumptions. First, the CSP 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 cipher text access control, hierarchical access control, access control based on fully homomorphic encryption [1][2] and access control based on attribute-based encryption (ABE). 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. The basic ABE 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 (PC). This means that an encryption operation which takes one minute on a computer will take about half an hour to finish on a mobile device. Furthermore, present solutions don't solve the user privilege change issue 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 issue 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.

III PROPOSED SYSTEM

To address this problem, in this paper, we propose a Lightweight Data Sharing Scheme (LDSS) for mobile cloud computing environment.

The main contributions of LDSS are as follows:
(1) We design an algorithm called LDSS-CP-ABE based on Attribute-Based Encryption (ABE) method to offer efficient access control over cipher text. Identify the issues in cloud system for data storage on cloud. Since data is not secure on cloud user can upload the data in encrypted format.

(2) We use proxy servers for encryption and decryption operations. In our approach, computational intensive operations in ABE are conducted on proxy servers, which greatly reduce the computational overhead on

client side mobile devices. Meanwhile, in LDSS-CP-ABE, in order to maintain data privacy, a version attribute is also added to the access structure. The decryption key format is modified so that it can be sent to the proxy servers in a secure way.

(3)We introduce lazy re-encryption and description field of attributes to reduce the revocation overhead when dealing with the user revocation issue.

(4) Finally, we develop a data sharing prototype framework based on LDSS. The experiments show that LDSS can greatly reduce the overhead on the client side. Such an approach is beneficial to implement a realistic data sharing security scheme on mobile phones. The results also show that LDSS has better performance compared to the existing ABE based access control schemes over cipher text.

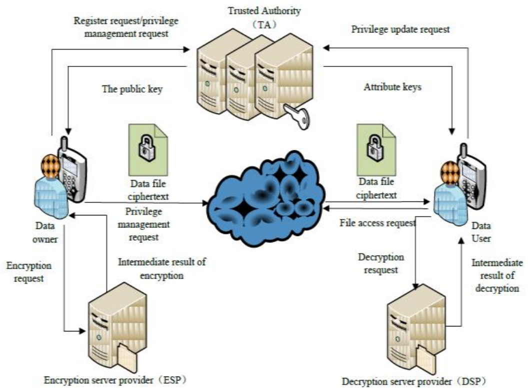
Register request/privilege management request
Trusted Authority (TA)
Privilege update request
The public key
Attribute keys
Data file ciphertext
Data file ciphertext
Privilege management request
File access request
Data owner
Data User
Encryption request
Intermediate result of encryption
Decryption resquest
Intermediate result of decryption
Encryption server provider（ESP）
Decryption server provider（DSP）

Fig:1. LDSS Framework

1. Text Encryption and Decryption: In this module user encrypted the plain text to encrypted format and uploaded to the cloud. The encryption is done by using a password. Only using this password only anyone can decrypt the information. The user upload the password also include with encrypted data. The trusted authority ID is responsible for passing the password to the requested user

2. Image Encryption and decryption: Like the same as the image encryption is also done. And the encrypted images and password will also be uploaded to the cloud. The trusted authority id is responsible for passing the password to the requested user.

3. Text request: Any user can view the file uploaded in the server. All the files are in encrypted format. User can’t view the files without know the password. For view the file first user need to request the password to Trusted Authority. The Authority checks the user and provides the password for valid user.

4. Image request: Image request is also same as the Text Request. The list of images can view in the application. But user can only view the images after getting the password from trusted authority.

5. View Encrypted Data: The user uploaded encrypted data can be view in the server side. The trusted authority act as server they have the responsibility to provide password for the requested user.

6. View user request: After user view the encrypted data they can request the password for encrypted data. This user request can be view in the trusted authority.

7. Provide password: After view the request Trusted authority validating the user and if the user is valid the Trusted authority provide password for the requested file via email. Using this password user can decrypt the file.

IV CONCLUSION

In recent years, many studies on access control in cloud are based on attribute-based encryption algorithm (ABE). However, traditional ABE is not suitable for mobile cloud because it is computationally intensive and mobile devices only have limited resources. In this paper, we propose LDSS to address this issue. It introduces a novel LDSS-CP-ABE algorithm to migrate major computation overhead from mobile devices onto proxy servers, thus it can solve the secure data sharing problem in mobile cloud. The experimental results show that LDSS can ensure data privacy 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 cipher text 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 Data. 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.

Author Details

P. Likitha Pursuing M.Tech at MJR College of Engineering & Technology, Department of CSE, Piler, Chittoor Dist.

Karamala Suresh Working as a Head of the Department in MJR College Of Engineering And Technology, Department Of Cse, Piler, Chittoor dist. He is having 14 years of teaching experience in engineering colleges, he received B.Tech(CSE) from JNTU

Hyderabad in 2002,Received M.E(CSE) from satyabama university Chennai in 2006,and Received M.Tech(CSE) in 2015 from JNTU Anantapuramu, he published several research papers in various national and international journals. He is interested in Computer Networks.