International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

COPY RIGHT

ELSEVIER SSRN

IJIEMR Transactions, online available on 22nd Jul 2019. Link :http://www.ijiemr.org/downloads.php?vol=Volume-08&issue=ISSUE-07

Title **ACHIEVING LIGHTWEIGHT SECURE DATA SHARING SCHEME FOR MOBILE CLOUD COMPUTING**

Volume 08, Issue 07, Pages: 256–262.

Paper Authors

V.KAMESWARI, B.RAMALINGA

SIR C.V. RAMAN Institute of Technology & Science, AP, India

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

ACHIEVING LIGHTWEIGHT SECURE DATA SHARING SCHEME FOR MOBILE CLOUD COMPUTING

V.KAMESWARI[1], B.RAMALINGA[2]
[1]PG Scholar, Dept of CSE, SIR C.V. RAMAN Institute of Technology & Science, AP, India
[2] Assistant Professor, Dept of CSE, SIR C.V. RAMAN Institute of Technology & Science, AP, 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 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.

1. INTRODUCTION

With increasing of the cloud storage and more usage of mobile has increased the data sharing model which have been used for the data retroviral and storage. As the usage of cloud have been increased widely, due to limitation of mobile storage. The cloud have more amount of storage and resources which is provide by the cloud service provider to store and share the data. The cloud mobile applications such as upload of photos, videos, documents and other files to the cloud and these files can be used to share with other users. Management functionality is also provided by the cloud service provider, but the personal information is important and it should be not shared in publically. It is important to provide the data privacy and the data security which is the major concern. The control mechanism provided by the cloud service provider is not sufficient as it does not meet the requirement of the data owner, the first and far most problem is whenever the user uploads the files on cloud then the cloud service provider may spy on the file for its use which cause the privacy problem later the user want to send the password for the encrypted files to unlock it. To overcome these problem data owner have to divide the data user into different user according to the

user who want to share their password to the particular group. Password management is a great issue for the security.

2. LITERATURE SURVEY

A cloud storage service allows data owner to outsource their data to the cloud and through which provide the data access to the users. Because the cloud server and the data owner are not in the same trust domain, the semi-trusted cloud server cannot be relied to enforce the access policy. To address this challenge, traditional methods usually require the data owner to encrypt the data and deliver decryption keys to authorized users. These methods, however, normally involve complicated key management and high overhead on data owner. In this paper, we design an access control framework for cloud storage systems that achieves fine-grained access control based on an adapted Ciphertext-Policy Attribute-based Encryption (CP-ABE) approach. In the proposed scheme, an efficient attribute revocation method is proposed to cope with the dynamic changes of users' access privileges in large-scale systems. The analysis shows that the proposed access control scheme is provably secure in the random oracle model and efficient to be applied into practice.

As the data produced by individuals and enterprises that need to be stored and utilized are rapidly increasing, data owners are motivated to outsource their local complex data management systems into the cloud for its great flexibility and economic savings. However, as sensitive cloud data may have to be encrypted before outsourcing, which obsoletes the traditional data utilization service based on plaintext keyword search, how to enable privacy-assured utilization mechanisms for outsourced cloud data is thus of paramount importance. Considering the large number of on-demand data users and huge amount of outsourced data files in cloud, the problem is particularly challenging, as it is extremely difficult to meet also the practical requirements of performance, system usability, and high-level user searching experiences. In this paper, we investigate the problem of secure and efficient similarity search over outsourced cloud data. Similarity search is a fundamental and powerful tool widely used in plaintext information retrieval, but has not been quite explored in the encrypted data domain. Our mechanism design first exploits a suppressing technique to build storage-efficient similarity keyword set from a given document collection, with edit distance as the similarity metric. Based on that, we then build a private trie-traverse searching index, and show it correctly achieves the defined similarity search functionality with constant search time complexity. We formally prove the privacy-preserving guarantee of the proposed mechanism under rigorous security treatment. To demonstrate the generality of our mechanism and further enrich the application spectrum, we also show our new construction naturally supports fuzzy search, a previously studied notion aiming only to tolerate typos and representation inconsistencies in the user searching input. The extensive experiments on Amazon cloud platform with real data set further demonstrate the validity and practicality of the proposed mechanism.

Data access control is an effective way to ensure data security in the cloud. However, due to data outsourcing and untrusted cloud servers, the data access control becomes a challenging issue in cloud storage systems. Existing access control schemes are no longer applicable to cloud storage systems, because they either produce multiple encrypted copies of the same data or require a fully trusted cloud server. Ciphertext-policy attribute-based encryption (CP-ABE) is a promising technique for access control of encrypted data. However, due to the inefficiency of decryption and revocation, existing CP-ABE schemes cannot be directly applied to construct a data access control scheme for multiauthority cloud storage systems, where users may hold attributes from multiple authorities. In this paper, we propose data access control for multiauthority cloud storage (DAC-MACS), an effective and secure data access control scheme with efficient decryption and revocation. Specifically, we construct a new multiauthority CP-ABE scheme with efficient decryption, and also design an efficient attribute revocation method that can achieve both forward security and backward security. We further propose an extensive data access control scheme (EDAC-MACS), which is secure under weaker security assumptions.

Attribute based proxy re-encryption scheme (ABPRE) is a new cryptographic primitive which extends the traditional proxy re-encryption (public key or identity based cryptosystem) to the attribute based counterpart, and thus empower users with delegating capability in the access control environment. Users, identified by attributes, could freely designate a proxy who can re-encrypt a ciphertext related with a certain access policy to another one with a different access policy. The proposed scheme is proved selective-structure chosen plaintext secure and master key secure without random oracles. Besides, we develop another kind of key delegating capability in our scheme and also discuss some related issues including a stronger security model and applications.

3. EXISTING SYSTEM:

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 attribute-based encryption (ABE). All these proposals are designed for non-mobile cloud environment Tysowski et al. considered a specific cloud computing environment where data are accessed by resource-constrained mobile devices, and proposed novel modifications to ABE, which assigned the higher computational overhead of cryptographic operations to the cloud provider and lowered the total communication cost for the mobile user.

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 CSP are either not sufficient or not very convenient. They cannot meet all the requirements of data owners. They consume large amount of storage and computation resources, which are not available for mobile devices Current solutions don't solve the user privilege change problem very well. Such an operation could result in very high

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

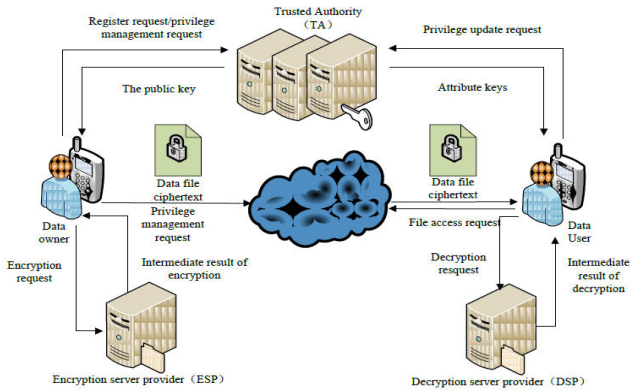
revocation cost. This is not applicable for mobile devices as well. Clearly, there is no proper solution which can effectively solve the secure data sharing problem in mobile cloud.

4. PROPOSED SYSTEM:

We propose a Lightweight Data Sharing Scheme (LDSS) for mobile cloud computing environment. The main contributions of LDSS are as follows: We design an algorithm called LDSS-CP-ABE based on Attribute-Based Encryption (ABE) method to offer efficient access control over ciphertext. 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. We introduce lazy re-encryption and description field of attributes to reduce the revocation overhead when dealing with the user revocation problem. Finally, we implement a data sharing prototype framework based on LDSS.

The experiments show that LDSS can greatly reduce the overhead on the client side, which only introduces a minimal additional cost on the server side. Such an approach is beneficial to implement a realistic data sharing security scheme on mobile devices. The results also show that LDSS has better performance compared to the existing ABE based access control schemes over ciphertext. Multiple revocation operations are merged into one, reducing the overall overhead In LDSS, the storage overhead needed for access control is very small compared to data files.

5.SYSTEM ARCHITECTURE:



6. IMPLEMENTATION:

System Framework:

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.In these applications, people (dataowners) can upload their documents andother files to the cloud and share these data with otherpeople (data users) they like to share. CSPs also providedata management functionality for data owners. Sincepersonal data files are sensitive, data owners are allowedto choose whether to make their data files public or canonly be shared with specific data users. Clearly, dataprivacy of the personal sensitive data is a big concern formany data owners.We propose LDSS, a framework of lightweight datasharing scheme in mobile cloud. It has thefollowing six components. (1)Data Owner (DO) (2) Data User (DU) (3) Trust Authority (TA) (4)

Encryption Service Provider (ESP) (5) Decryption Service Provider (DSP) (6) Cloud Service Provider (CSP).

Data Owner (DO):

When the data owner (DO) registers on TA, TA runs the algorithm Setup() to generate a public key PK and a master key MK. PK is sent to DO while MK is kept on TA itself. DO defines its own attribute set and assignsattributes to its contacts. All these information will be sent to TA and the cloud.TA and the cloud receive the information and storeit.DO uploads data to the mobilecloud and share it with friends. DO determines the accesscontrol policies.DO sends data to the cloud. Sincethe cloud is not credible, data has to be encrypted before it is uploaded. The DO defines access control policy in the form of access control tree on data files to assign which attributes a DU shouldobtain if he wants to access a certain data file.

Data User (DU):

DU logins onto the system and sends, an authorization request to TA. The authorization request includes attribute keys (SK) which DU already has.TA accepts the authorization request and checks the request and a generate attribute keys (SK)for DU.DU sends a request for data to the cloud.Cloud receives the request and checks if the DU meets the access requirement. DU receives the ciphertext, which includesciphertext of data files and ciphertext of the symmetric key. DU decrypt the ciphertext of the symmetric key with the assistance of DSP. DU uses the symmetric key to decrypt the ciphertext of data files.

Trusted Authority:

To make LDSS feasible in practice, a trustedauthority (TA) is introduced. It is responsible ofgenerating public and private keys, and distributingattribute keys to users. With this mechanism, users can share and access data without being aware of the encryption and decryption operations. We assume TA is entirely credible, and a trusted channel exists between the TA and every user. The fact that a trusted channel exists doesn't mean that the data can be shared through the trusted channel, for the data can be in a large amount. TA is only used to transfer keys (in a small amount) securely between users. In addition, it's requested that TA is online all the time because data users may access data at any time and need TA to update attribute keys.

Cloud Service Provider:

CSP stores the data for DO. It faithfully executes the operations requested by DO, while it may peek over data that DO has stored in the cloud.DU sends a request for data to the cloud. Cloud receives the request and checks if the DU meets the access requirement. If DU can't meet the requirement, it refuses therequest; otherwise it sends the ciphertext to DU. CSP manages the Uploaded Files.

7. 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 ciphertext retrieval over existing data sharing schemes.

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: DACMACS: Effective Data Access Control for Multiauthority Cloud Storage Systems. IEEE Transactions on Information Forensics and Security, Vol. 8, No. 11, pp.1790-1801, 2013.

[13] Stehlé D, Steinfeld R. Faster fully homomorphic encryption. in: Proceedings of 16th International Conference on the Theory and Application of Cryptology and

Information Security. Singapore: Springer press, pp.377-394, 2010.

[14] Junzuo Lai, Robert H. Deng ,Yingjiu Li ,et al. Fully secure keypolicy attribute-based encryption with constant-size ciphertexts and fast decryption. In: Proceedings of the 9th ACM symposium on Information, Computer and Communications Security (ASIACCS), pp. 239-248, Jun. 2014.

[15] Bethencourt J, Sahai A, Waters B. Ciphertext-policy attribute based encryption in: Proceedings of the 2007 IEEE Symposium on Security and Privacy (SP). Washington, USA: IEEE Computer Society, pp. 321-334, 2007.