ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 4, April 2018

A Featherweight Guarded File Distribution Scheme in Mobile Cloud Computing

[1] Sree Vidhya Valluri, [2] Dr.P.Chitti Babu, [3] D.Sudhakar
[1] Dept of MCA ,APGCCS, [2] Principal, APGCCS,[3] Assoc Prof, APGCCS

Abstract: Nowadays, Cloud Computing is found with huge popularity. So people are getting accustomed to new era of File Distribution. Now, this is also required for mobiles. By using this mobile cloud computing we can share or access files at any time from any place. For secured Cloud Computing, we propose the new File distributing scheme in Mobile Cloud Computing. Owner files should be guarded before uploading them to the cloud. The main scope of this project is to adopt Cipher text Policy Attribute Based Encryption (CP-ABE), an access control technology and also this Featherweight Guarded File Distribution (FGFD) moves a heavy portion of access control tree transformation in CP-ABE to proxy servers. The provisional result shows that FGFD can reduce the load on the mobiles, especially when users are distributing files in mobile cloud environments.

Index Terms- Featherweight Guarded File Distribution, Cipher text Policy Attribute Based Encryption

1. INTRODUCTION

This era is completely adapted to new technologies; various cloud mobile applications have been widely used. In these applications, people can distribute their files to the cloud and share them with other people, whom they like. Cloud also provides data management functionality for data owners. As the files are sensitive to distribute, Access control policies are maintained by the File Owner. The resources provided by the Cloud are not suitable for mobile devices. They cannot meet all the requirements of owners. For example: first, when people distribute their files through the cloud, they are distributing their files in a place where the security is completely not in the hands of file owner, and the Cloud may attack on files for its commercial interests or for other reasons. Next, people have to send password to each user if they only want to distribute the encrypted data with authorization, which is very difficult process. To simplify the access management, the file owner can divide users into different sections and send password to the sections to whom they want to distribute the files. In both cases, password management is a big setback.

To solve these problems, owner's files should be guarded before distributing them through the cloud, so that the file is guarded against the Cloud. The file guarding brings new problems. How to provide guard on ciphertext decryption so that only the authorized users can access the file. It is challenging. Along with this, system must provide file owners effective user access control, so they can grant/revoke file access easily on the file users. There have been several researches undergone on this issue. In these researches, they have the following assumptions. First, the Cloud is considered as honest. Second, all the files are guarded before distributing to the Cloud. Third, user authorization on certain data is achieved through key distribution.

2. LITERATURE SURVEY

1) Attribute-based fine-grained access control with efficient revocation in cloud storage systems
AUTHORS: Kan Yang, Xiaohua Jia, Kui Ren

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.

2) Achieving Usable and Privacy-assured Similarity Search over Outsourced Cloud Data
AUTHORS: Cong Wang, Kui Ren, Shucheng Yu, and Karthik Mahendra Raje

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 4, April 2018

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.

3)DACMACS: Effective Data Access Control for Multiauthority Cloud Storage Systems

AUTHORS: Kan Yang, Xiaohua Jia, Kui Ren, Bo Zhang, Ruitao Xie

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.

4) Attribute based proxy re-encryption with delegating capabilities.

AUTHORS: Liang Xiaohui, Cao Zhenfu, Lin Huang

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.also discuss some related issues including a stronger security model and applications.

3. PROBLEM DESCRIPTION

Generally, we can divide these approaches into four categories: simple cipher text access control, hierarchical access control, access control based on fully homomorphic encryption and guarded based on attribute-based encryption (ABE). All these are designed for only 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

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 4, April 2018

the cloud provider and lowered the total communication cost for the mobile user.

4. METHODOLOGY ADOPTED

We propose FGFD, a framework of Featherweight File Distributing Scheme in mobile cloud computing. It has the following six components. Data Owner (DO): DO shares files to the mobile cloud and share it with users. Owner determines the access control Mechanisms. Data User (DU): DU access files from the mobile cloud. Trust Party (TP): TP is responsible for creating and distributing keys Encryption Service Provider (ESP): ESP converts our files to non understandable format Decryption Service Provider (DSP): DSP converts non understandable format to understandable format Cloud: Cloud stores the data for DO. It honestly performs the actions given by the DO

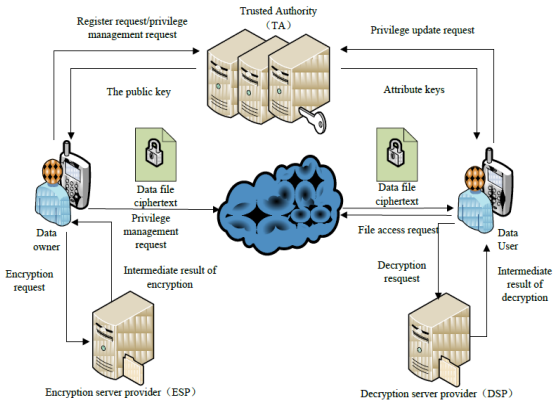

Fig1: System Architecture

5. EXPERIMENTAL AND EVALUATION

Attribute Description Field in FGFD-CP-ABE

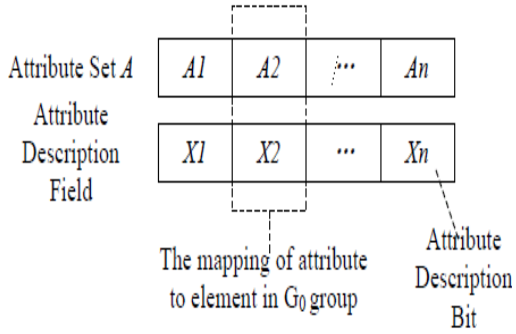

Fig2: Attribute description field of DO

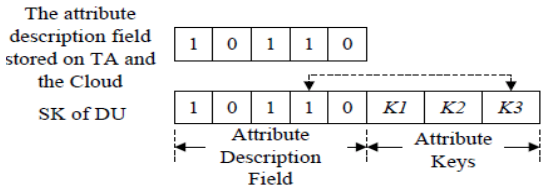

Fig3: Attribute description field of DU

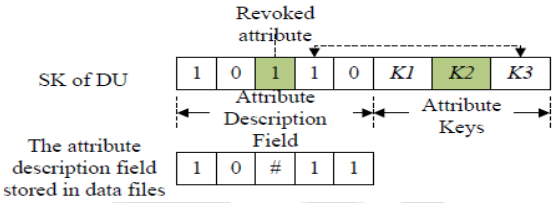

Fig4: Attribute description field of data files

Attribute description field is introduced in FGFD for user access management. It keeps guarded accessing of file. To better illustrate the attribute description field, we have the following definitions.

DEFINITION 1: ATTRIBUTE DESCRIPTION FIELD. Attribute description field is a string of binary bits, which describes attribute information related to DO, DU and data files.

DEFINITION 2: ATTRIBUTE DESCRIPTION BIT. Attribute description bit is every bit in Attribute description field corresponding to an attribute.

There are three kinds of Attribute Description fields, namely, the Attribute Description field of DO, the attribute description field of DU and the attribute description field of data file.

The attribute description field of DO is generated by the TP. When a data owner registered with TP, it sends its own attribute set to TP. TP then generates attribute description field, in which each attribute bit represents a value. TP keeps the attribute description field in the DO-PK/MK-information table. The attribute description field of DO is shown in fig2. The attribute description field of a data user (DU) is generated by TP and the cloud under the supervision of the data owner. TA and the cloud keep it in contacts-information table. TP and the cloud keep up-to-date information of DU's attribute description fields according to the data owner. Each data user also maintains an attribute description field which may contains out-dated control information. Data users obtain

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 4, April 2018

their attribute description fields from TP when TP generates attribute keys for them. The attribute description field is sent together with the attribute keys. In the attribute description field of DU, every bit is either 1 or 0. A 1 denotes that the DU owns the attribute while a 0 denotes the opposite. For example, if the data owner has 5 attributes, a sample attribute description field is generated.

The attribute description field of data files is stored on DO. It represents which attributes are assigned in data files' access control policy. If an attribute is included in the access control policy, the corresponding bit in the description field is 1, otherwise it's 0. '#' may appear in the attribute description field when an attribute is included in the access control policy and some data users have this attribute revoked. For a data owner who has five attribute.

6. RESULTS AND DISCUSSION

FGFD scheme is designed for file distributing in mobile cloud. The whole process of FGFD includes system initialization, file distributing, user authorization, and file access operations. It also has to support attribute revocation and file update operations.

6.1 FILE DISTRIBUTING

The process of file sharing encrypts data files. The specific process is described as follows.
1. DO select a file M which is to be uploaded and encrypts it using a symmetric cryptographic mechanism with a symmetric key K, generating cipher text C.
2. DO assign access control policy for M and encrypts K with the assistance of ESP, generating the cipher text of K (CT).
3. DO upload C, CT and access control policy to the cloud.

6.2 USER AUTHORIZATION

The process of user authorization generates attribute keys for data users. The specific process is described as follows.
1. DU logins onto the system and sends, an authorization request to TP. The authorization request includes attribute keys (SK) which DU already has.
2. TP accepts the authorization request and checks whether DU has logged on before. If the user hasn't logged on before, go to step 3 otherwise go to step (4).
3. TP generates attribute keys (SK) for DU.
4. TP 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), otherwise go to step (6).
5. For each inconsistent bit in description field, if it is 1 on data user's side and 0 on TP's side, it indicates that DU's attribute has been revoked, and then TP does nothing on this bit. If it is reversed scenario, it indicates that DU has been assigned with a new attribute, and then TP generates the corresponding attribute key for DU.
6. TP checks the version of every attribute key of DU. If it's not the same with the current version, then TP updates the corresponding attribute key for DU.
At the stage of user authorization, TP updates attribute keys for DU according to the attribute description field, which is stored with SK. It describes which attributes DU has and their corresponding versions. TP also keeps attribute description field of DU in database. When DO changes the attribute of DU, the attribute description field on the TP side is also updated. Thus, when DU logins on the system, the attribute description field on itself may be different from that of TP. TP has to update the attribute keys for DU according to the attribute description field just as described above.

6.3 ACCESS FILES

When DU requests to access a certain data file, the specific process is described as follows:
1. DU sends a request for data to the cloud.
2. Cloud receives the request and checks if the DU meets the access requirement. If DU can't meet the requirement, it refuses the request; otherwise it sends the cipher text to DU.
3. DU receives the cipher text, which includes cipher text of data files and cipher text of the symmetric key. Then DU decrypts the cipher text of the symmetric key with the assistance of DSP.
4. DU uses the symmetric key to decrypt the cipher text of data files.

6.4 STORAGE BURDEN EVALUATION

We also evaluate the storage overhead of FGFD and compare it with existing CP-ABE schemes.

MEASUREMENT OF STORAGE OVERHEAD OF FGFD
FGFD is based on 160-bit elliptic curve group, which is derived from the super singular curve $y2=x3+x$ over a 512-bit finite field. The size of LG0, LG1, LZ is 40B, 64B and 20B, separately. In FGFD, the storage overhead needed for access control is the storage of PK/MK, SK and CT. PK and MK is 156B and 888B separately. The size of CT grows with the number of attributes in access

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 4, April 2018

control policy and the size of SK grows with the number of attributes in DU's attribute set.
When sharing data files, the symmetric key itself is encrypted by CP-ABE. Since the size of data files remains the same after encryption, we only evaluate the size change of the symmetric key. After encryption when the number of attributes in access control policy is 1, 2, 4, 8, 16 and 32. It can be concluded that the size of cipher text rises with the number of attributes in access control policy in both BSW CP-ABE and FGFD. The size of symmetric key cipher text of BSW CP-ABE is a little bigger than that of FGFD. When the number of attributes rises to 32, the size of symmetric key cipher text is smaller than 10KB in both schemes, which is very small compared to the data files. For DU authorization, the size of SK is linear with the number of attributes in DU's attribute set. Shows the size of SK when the number of attributes in DU's attributes set is 2, 4, 8 and 32, respectively. In sum, in FGFD, the storage overhead needed for access control is very small compared to data files.

7. CONCLUSIONS

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 FGFD to address this issue. It introduces a novel FGFD-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 FGFD 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.

8. REFERENCE BOOKS

[1] 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.

[2] 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

[3] 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.

[4] Liang Xiaohui, Cao Zhenfu, Lin Huang, et al. Attribute based proxy re-encryption with delegating capabilities. in: Proceedings of the 4th International Symposium on Information, Computer and Communications Security. New York, NY, USA: ACM press, pp. 276-286, 2009.