International Journal For Technological Research In Engineering
Volume 6, Issue 9, May-2019 *ISSN (Online): 2347 - 4718*

A LIGHTWEIGHT SECURE DATA SHARING SCHEME FOR MOBILE CLOUD COMPUTING

Nirmala Ganigar[1], A Sumitra[2], Chaitra Lakshmi Krishna[3], Dugudala Ramya[4], N. Prathibha[5]
[1]Asst. Professor, [2,3,4,5]B.E Student
Dept of Computer Science, Ballari Institute of Technology & Management

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.

Keywords: Cloud computing, data privacy, data security, encryption, data sharing, access control.

I. INTRODUCTION

Cloud computing means storing data and accessing that data from 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. Sharing of data over the cloud is the new trend that is being set on. The amount of data generated on a day to day life is increasing and to store that all of the data in traditional hardware is not possible because of limited storage capacity. Therefore, transferring the data to the cloud is a necessity where the user can get unlimited storage. Security of that data over is the next big concern for most of us. After uploading the data to the cloud use loses its control over that data. Since personal data files are sensitive, data owners are allowed to share data files with data users by generating a random key. Therefore, privacy of the personal sensitive data is a big concern for many data owners. Nowadays, various cloud mobile applications have been widely used. In this applications, people(data owners) can upload there documents and other files to the cloud and share these data with other people(data user) they like to share. CSPs also provide data management functionality for data owners. Clearly, data privacy of the personal sensitive data is big concern for many data owners.

II. LITERATURE SURVEY

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.

Cong Wang, Kui Ren, Shucheng Yu, and Karthik Mahendra Raje

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.

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.

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.

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.

III. EXISTING SYSTEM

In general, we can divide these approaches into accustomed to a new era of data sharing model in which four categories: simple ciphertext access control, the data is stored on the cloud and the mobile devices hierarchical access control, access control based on are used to store/retrieve the data from the cloud. In fully homomorphic encryption and access control these applications, people (dataowners) can upload their based on attribute-based encryption (ABE). All these documents and other files to the cloud and share these proposals are designed for non-mobile cloud data with other people (data users) they like to share. Environment CSPs also provide data management functionality for
Ø Tysowski et al. considered a specific cloud data owners. Since personal data files are sensitive, data Computing where data are accessed by resource-owners are allowed to choose whether to make their data constrained mobile devices, and proposed novel files public or can only be shared with specific data users. modifications to ABE, which assigned the higher Clearly, data privacy of the personal sensitive data is a computational overhead of cryptographic operations big concern for many data owners. We propose LDSS, a to the cloud provider and lowered the total framework of lightweight data sharing scheme in mobile communication cost for the mobile user. cloud. It has the following six components. (1)Data

IV. PROPOSED SYSTEM

We propose a Lightweight Data Sharing Scheme (LDSS) for mobile cloud computing environment 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.

DESIGN
SYSTEM ARCHITECTURE

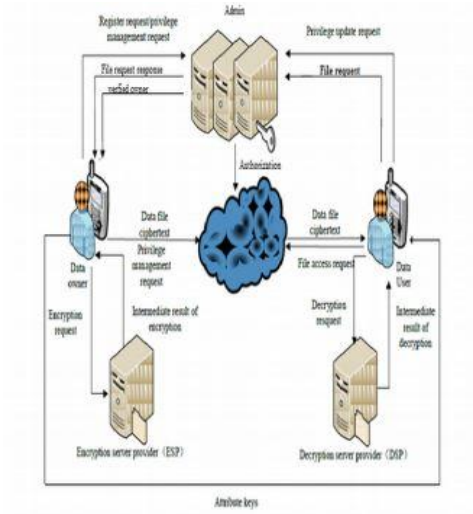


Figure 2: System Architecture

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 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 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. We propose LDSS, a framework of lightweight data sharing scheme in mobile cloud. It has the following 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).

IMPLEMENTATION AND SNAPSHOTS

The system is implemented with the following Modules.

Data Owner (DO) Once the Owner enters into the application he/she has to register. If the owner is already registered then he/she can login using their login credentials. Before login the owner as to be verified by the admin after registering. Now the owner will send the access request to the admin, if the admin accepts the request then he can upload the files to the database. All these information will be sent to admin and the cloud. Admin and the cloud receive the information and store it. DO determines the access control policies. DO sends data to the cloud. Since the 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 should obtain if he wants to access a certain data file.

Data User (DU):

Once the User enters into the application he/she has to register. If the user is already registered then he/she can login using their login credentials. Before login the user as to be verified by the admin. DU logins onto the system and sends, an access request to Admin. Admin activates the request then user can view the encrypted file uploaded by the owner. Now user request for decryption key to download the files. When the key is sent then, 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.

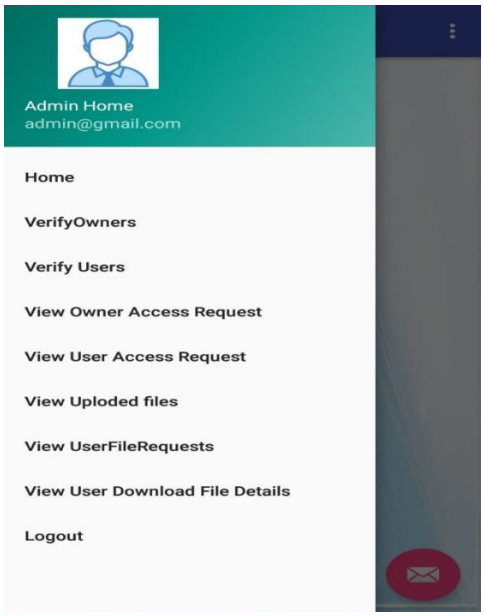
Admin:

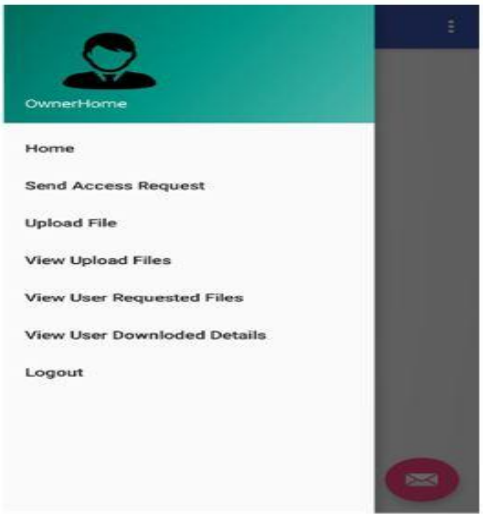
To make LDSS feasible in practice, a Admin is introduced. It is responsible for activation and deactivation of the keys, and distributing attribute keys response to the owner. With this mechanism. users can share and access data without being aware of the encryption and decryption operations.We assume Admin is entirely credible, and a trustedchannel exists between the Admin 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. Admin is only used for activation between users. In addition, it's requested that Admin is online all the time because data users may access data at any time and need Admin to activate the requests.

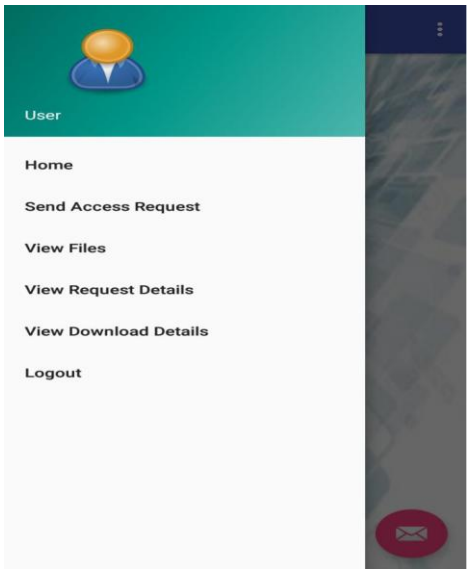
Cloud Service Provider:

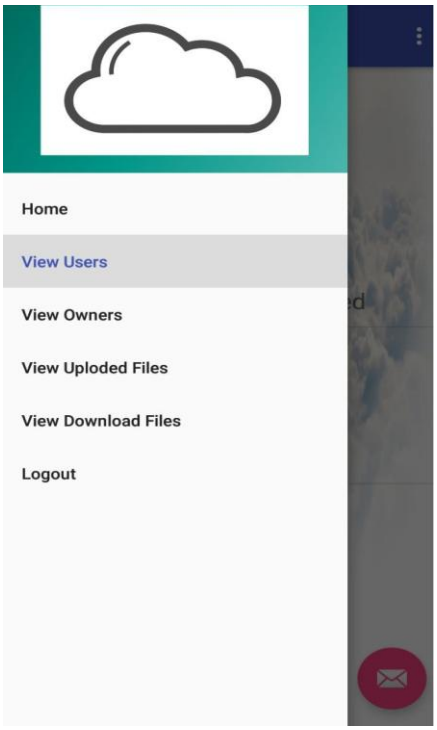
CSP stores the data for DO. It faithfully executes the operations requested by DO, while it may peek over data that DO has stored in the cloud. DU sends a request for data to the cloud. Cloud receives the request and checks if the DU meets the access requirement. If DU can't meet the requirement, it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

Figure 3: Snapshots of the Project.









V. 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.

VI. FUTURE SCOPE

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] 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.

[7] 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

