

## A Lightweight Secure Data Sharing Scheme for MobileCloud Computing

### 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.

### 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.

### **DISADVANTAGES OF EXISTING SYSTEM:**

- ❖ 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 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.

### **PROPOSED SYSTEM:**

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

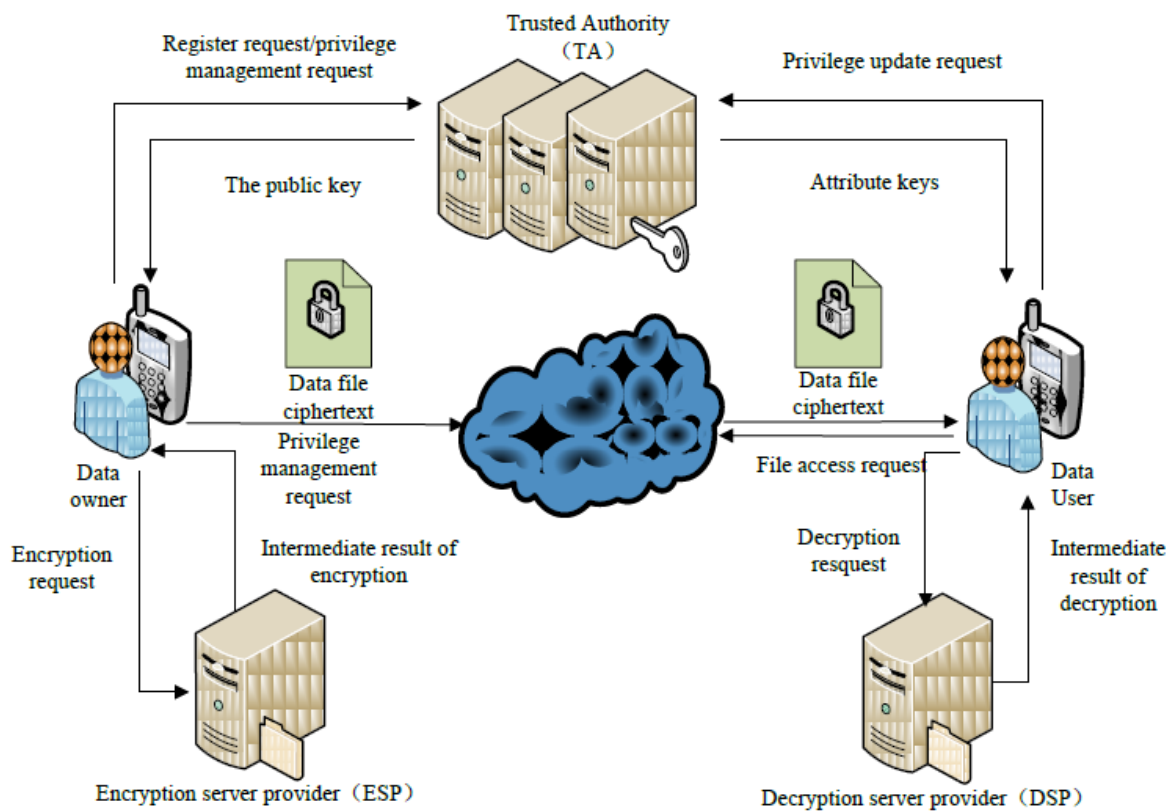
- ❖ The main contributions of LDSS are as follows:
- ❖ We design an algorithm called LDSS-CP-ABE based on Attribute-Based Encryption (ABE) method to offer efficient access control over ciphertext.
- ❖ We use proxy servers for encryption and decryption operations. In our approach, computational intensive 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.

#### **ADVANTAGES OF PROPOSED SYSTEM:**

- ❖ 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.

## SYSTEM ARCHITECTURE:



## **SYSTEM REQUIREMENTS:**

### **HARDWARE REQUIREMENTS:**

- System : Pentium Dual Core.
- Hard Disk : 120 GB.
- Monitor : 15” LED
- Input Devices : Keyboard, Mouse
- Ram : 1 GB

### **SOFTWARE REQUIREMENTS:**

- Operating system : Windows 7.
- Coding Language : JAVA/J2EE
- Tool : Netbeans 7.2.1
- Database : MYSQL

### **REFERENCE:**

Ruixuan Li, *Member, IEEE*, ChenglinShen, Heng He, ZhiyongXu, and Cheng-ZhongXu, *Member, IEEE*, “A Lightweight Secure Data Sharing Scheme for Mobile Cloud Computing”, **IEEE Transactions on Cloud Computing, 2017.**