# MOBILE CLOUD COMPUTING BASED A LIGHTWEIGHT DATA SHARING SCHEME USING CP-ABE

[#1]S SOMASEKHAR., MTECH-CSE., ASSISTANT PROFESSOR,
[#2]V LEENA PARIMALA., MTECH-CSE., ASSISTANT PROFESSOR,
([#3]M MADHU LATHA.,METCH-CSE., ASSISTANT PROFESSOR .

**ABSTRACT:** The ubiquity of distributed computing, cell phones can stock and recover sensitive data from cloud whenever. Therefore, the information security issue in versatile cloud tries out to be increasingly extreme and forestalls advance improvement of portable cloud. There are generous examinations that have been run to enhance the cloud security. Be that as it can, a big slice of them are not relevant for versatile cloud since cell phones just have constrained registering assets and power. Arrangements with low computational upstairs are in awesome requirement for versatile cloud applications. In this project, we suggest a lightweight data sharing scheme (LDSS) for portable distributed computing. It embraces CP-ABE, an entrance control innovation utilized as a part of typical cloud condition, yet changes the construction of access regulator tree to make it reasonable for portable cloud conditions. LDSS moves an extensive section of the computational genuine access control tree change in CPABE from mobiles to outside go-between servers. Moreover, to decrease the client repudiation cost, it acquaints quality portrayal fields with execute lethargic disavowal, which is a prickly issue in program based CP-ABE substructure. The exploratory outcomes demonstrate that LDSS can successfully lessen the overhead on the cell phone side when clients are sharing information in portable cloud conditions.

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

## I. INTRODUCTION

In 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 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. 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. First, when people upload their data files onto the cloud, they are leaving the data in a place where is out of their control, and the CSP may spy on user data for its commercial interests and/or other reasons. Second, people have to send password to each data user if they only want to share the encrypted data with certain users, which is very cumbersome. To simplify the privilege management, the data owner can divide data users into different groups and send password to the groups which they want to share the data. However, this approach requires finegrained access control. In both cases, password management is a big issue. 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, version attribute is also needed to maintain data privacy, version attribute is also added to 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 cipher text. The rest of this paper is organized as follows. • section 2 presents some fundamental concepts in secure mobile cloud data sharing and the security premise section 3 gives the detailed design of LDSS. • Section 4 and section 5 gives the safety assessment and performance evaluation, respectively. • Section 6 presents related works. Finally, section 7 concludes our work with the future works. Apparently, to solve the above problems, personal sensitive data should be encrypted before uploaded onto the cloud so that the data is secure against the CSP. However, the data encryption brings new problems.

How to provide efficient access control mechanism on cipher text decryption so that only the authorized users can access the plaintext data is challenging. In addition, system must offer data owner's effective user privilege management capability, so they can grant/revoke data access privileges easily on the data users. There have been substantial researches on the issue of data 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 holomorphic encryption [1] [2] and access control based on attribute-based information. All these proposals are designed for nonmobile cloud environment. They consume large amount of storage and computation resources, which are not available for mobile devices. According to the experimental results in [26], 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 PC will take about half an hour to finish on a mobile device. Furthermore, 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. As the mobile cloud becomes more and more popular, providing an efficient secure data sharing mechanism in mobile cloud is in urgent need.

## II. PROBLEM DEFINITION

### 2.1 Preliminary Techniques

### 2.1.1 Lazy re-encryption

In ciphertext access control, data needs to be reencrypted when some users' access privileges to the data are revoked. However, frequent reencryption brings heavy computational overhead, and the accessed plain text data may already be stored on these data users. Therefore, this paper adopts lazy re-encryption method proposed in with lazy re-encryption, when a users' access privilege is revoked, data is not re-encrypted until the data owner updates the data.in ur approach, when the data owner revokes a user's privilege, the file of the access control policy that contains these attributes will be marked. Later, when the data owner updates this file, it first checks the mark to see if it has been marked as revoked. If that is the case this file will be re-encrypted.

### 2.1.2 Attribute-Based Encryption

Attribute-based encryption (ABE) is proposed by Sahai and Waters [29]. It is derived from the Identity- Based Encryption (IBE) and is particularly suitable for one-to-many data sharing scenarios in a distributed and open cloud environment. Attribute-based encryption is divided into two categories: one is the Cipher text-Policy Attribute Based Encryption (CP-ABE), in which the access control policy is embedded into cipher text; the other one is Key-Policy Attribute Based Encryption (KP-ABE), in which the access control policy is embedded in the user's key attributes. In real applications, CP-ABE is more suitable since it resembles role-based access control. In CP-ABE, the data owner designs the access control policy and assigns attributes to data users. A user can decrypt the data properly if the user's attributes satisfy the access control policy.

## III.SYSTEM DESCRIPTION

We propose LDSS, a framework of lightweight data-sharing scheme in mobile cloud (see Fig. 1). It has the following six components. (1)Data Owner (DO): DO upload data to the mobile cloud and share it with friends. (2)Data User (DU): DU retrieves data from the mobile cloud. (3)Trust Authority (TA): TA is responsible for generating and distributing attribute keys. (4)Encryption Service Provider (ESP): ESP provides data encryption operations for DO. (5)Decryption Service Provider (DSP): DSP provides data decryption operations for DU. (6)Cloud Service Provider (CSP): CSP stores the data for DO. It faithfully executes the operations requested by DO, while it may peek over data that DO have stored in the cloud. As shown in Fig. 1, a 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. In LDSS, data files are all encrypted with the symmetric encryption mechanism, and the symmetric key for data encryption is also encrypted using attribute based encryption (ABE). The access control policy is embedded in the cipher text of the symmetric key. Only a DU who obtains attribute keys that satisfy the access control policy can decrypt the cipher text and retrieve the symmetric key. As the encryption and decryption are both computationally intensive, they introduce heavy burden for mobile users. To relieve the overhead on the client side mobile devices, encryption service provider (ESP) and decryption service provider (DSP) are used. Both the encryption service provider and the decryption service provider are also semitrusted. We modify the traditional CP-ABE algorithm and design an LDSS- CP-ABE algorithm to ensure the data privacy when outsourcing computational tasks to ESP and DSP. As the encryption and decryption are both computationally intensive, they introduce heavy burden for mobile users.to relieve the overhead on the client side mobile devices,encryption service provides(ESP) and decryption service provider(DSP) are used. Both the encryption service provider and the decryption service provider are used.

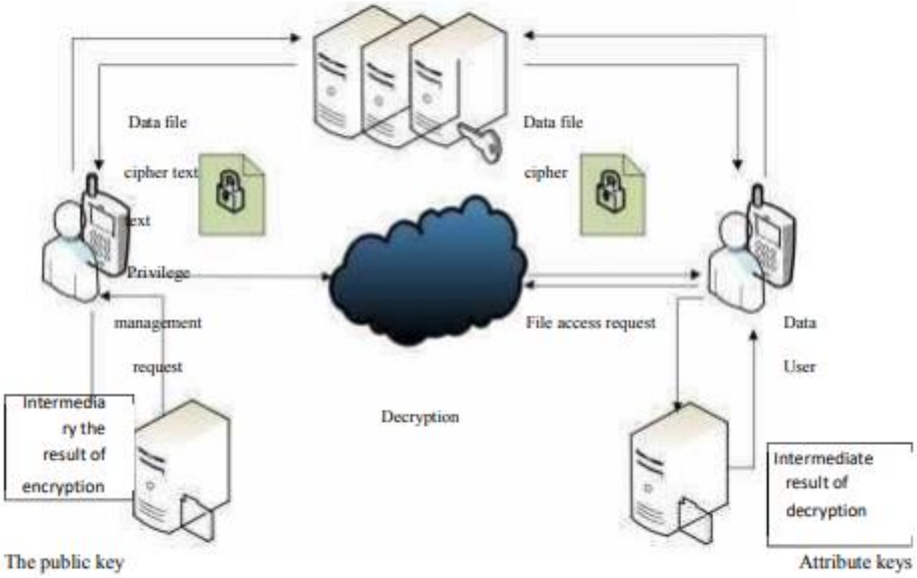

Fig. 1. A lightweight data-sharing scheme (LDSS) framework.

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 TA.when a data owner registered with TA, it sends its own attribute set to TA.TA then generates attribute description field, in which each attribute bit represents a value in G0.TA keeps the attribute description field in the DO –PK/MK-information table. The attribute description field of the data user is generated by TA and the cloud under the supervision of the data owner.TA and the cloud keep it in contacts information table.TA and the cloud keep upto date information of DU attribute description field which may contain out dated control information.

## IV.METHODOLOGIES

In this paper we propose some methodologies to acheive the goal that is to kind the sharing data will be secure.

**4.1 DES ALGORITHM:** Similarly with most encryption designs, DES expects two well- springs of information - the plaintext to be mixed also, the riddle key. The manner by which the plaintext is recognized, and the key strategy used for encryption and unscrambling, both choose the sort of figure it DES is a usage of a lucifer Cipher. It utilizes 16 round lucifer creation. The structure proportion is 64-bit. In any case, key length is 64-bit, DES has an influencing key length of 56 bits,since 8 of the 64 bits of the principal enter are not in the usage by the encryption count (work as check bits allegorically)

**4.2 ABE ALGORITHM**: Quality based encryption (ABE) is a respectably late approach that reconsiders open key cryptography. In customary open key cryptography, a message is encoded for a particu-lar beneficiary utilizing the expert's open key. Identity established cryptography and particularly character based encryption (IBE)changed the standard perception of open key cryptography by empowering individuals when all is said in done key to be an optional string, e.g., the electronic post address of the client.ABE goes well past and depicts the personality not nuclear yet rather as a blueprint of properties e.g., parts, and messages can be encoded with regard to subsets of characteristics (key-technique ABE - KP-ABE) or strategies depicted over a course of action of attributes(ciphertext- approach). The key issue is, that some individual should simply have the ability to arrange a ciphertext in the event that the individual holds a key for "organizing properties" (more underneath) where customer keys are always issued by some place stock in party

### 4.3CP-ABE ALGORITHM

In ciphertext-framework unmistakable based encryption a client's private-key is associated with an arranging of charecters and a ciphertext chooses a path system over a depicted universe of properties inside the structure.k arranged of n credits must be available (there may in like way be non-monotone access approaches with extra negations and in the interim there are more- over upgrades for strategies depicted as discretionary circuits).For example, let us expect that the universe of credits is depicted to be A,B,C,D and client 1 gets a key to properties A,B and client 2 to property D.On the off irregular that a ciphertext is changed over concerning the strategy (A?C)?D, by then client 2 will be able to mastermind, while client 1 won't have the fitness to interpret. Calculation starting now and into the foreseeable future licenses to see got a handle on guaranteeing, i.e., bolster is joined into the mixed data and essentially people who satisfy the related course of action can arrange data. Another dazzling highlights is, that clients can get their safe keys after information has been mixedSo information can be blended without learning of the honest to goodness procedure of customers that will have the capacity to unscramble, yet simply picking the system which honors to unravel. Any future customers that will be given a key with respect to properties to such a degree, to the point that the approach can be ful?lled will by then can translate the data.

## V.CONCLUSION:

In recent years, many studies on access control in cloud are based on attributebased encryption (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 a major computational overhead from mobile devices into proxy servers, thus it can solve the secure data sharing problem in mobile cloud. The experimental results show that LDSS can ensure data privacy problem in mobile cloud and reduces the overhead on the user side in the mobile cloud.

## REFERENCES

[1] 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

[2] Pirretti M, Traynor P, McDaniel P, et al. Secure atrribute-based systems. In: Proceedings of the 13th ACM Conference on Computer and Communications Security. New York USA: ACM press, pp. 99-112, 2006.

[3] Sandhu R S, Coyne E J, Feinstein H L, et al. Role-based access control models. Computer, 29(2):38-47, 1996.

[4] Di Vimercati S D C, Foresti S, Jajodia S, et al. Over-encryption: management of access control evolution on outsourced data. In: Proceedings of the 33rd international conference on Very large data bases. Vienna, Austria: ACM, pp. 123-134, 2007

[5] Kan Yang, Xiaohua Jia, Kui Ren, Ruitao Xie, and Liusheng Huang: Enabling efficient access control with dynamic policy updating for big data in the cloud. INFOCOM 2014, pp.2013-2021, 2014

[6] Zhou Z, Huang D. Efficient and secure data storage operations for mobile cloud computing. In: Proceedings of 8th International Conference on Network and Service Management (CNSM 2012), Las Vegas, USA: IEEE, pp. 37-45, 2012.