# ABE Based Lightweight Secure Re-Encryption Scheme for Mobile Cloud Data Sharing

*Sreelekshmi A Krishna*[1]

[1]PG Student
[1] Department of Computer Science
[1]Sree Ayyappa College (TDB),Chengannur, India

***Abstract :*** *With the popularity of cloud computing, mobile devices can store or 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 ABE based lightweight Secure Re-encryption scheme for MC data sharing (LRE-MCDS) for mobile cloud computing environment. 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. LRE-MCDS 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 LRE-MCDS can effectively reduce the overhead on the mobile device side when users are sharing data in mobile cloud environments. In this proposed we are using a combination of Attribute-Based Encryption and Rivest Cipher -6(RC-6) Algorithm for encrypting the data before sending it to the cloud. This will help the user to securely store and share the data in encrypted form.*

***Index Terms*** **-** Mobile Cloud Computing**,** Data Encryption, Access Control, User Revocation, Data Privacy, Data Security, Data Sharing**..**

## I. INTRODUCTION

Nowadays, mobile devices like smartphones and tablets are increasingly becoming an essential part of human life as they are the most effective and convenient communication tools not bounded by time and place. Such devices are quickly raising popularities due to the support for a wide range of applications like gaming, image processing, video processing and online social network services that allow users to accumulate rich experience. Such applications include iPhone apps and Google apps, which run on the devices and/or on remote servers via wireless networks. The rapid progress of mobile computing becomes a powerful trend in the development of IT technology as well as commerce and industry fields. However, the mobile devices are facing many challenges in their resources like battery life, storage, and bandwidth. Furthermore, they are also facing communication challenges such as mobility and security [1]. Such limitations have significantly affected on the improvement of service qualities.

On the other hand, with the emerging technology of cloud computing, more and more services have been offered and delivered through the Internet. Cloud computing offers tremendous advantages by allowing users to use its infrastructure like servers, networks, and storages, platforms such as middleware services and operating systems, and software like application programs. All of those services are provided by Cloud Service Providers (CSPs) like Google, Amazon, and Salesforce at low costs. In addition, cloud computing enables users to elastically utilize resources in an on-demand fashion. As a result, mobile applications can be rapidly provisioned and released with the minimal management efforts or service providers' interactions. With the explosion of mobile applications and the support of cloud computing for a variety of services for mobile users, mobile cloud computing is introduced as an integration of cloud computing into the mobile environment. Mobile cloud computing brings new types of services and facilities for mobile users to take full advantage of cloud computing.

In order to leverage such a technology and services, mobile users need to outsource their data to the CSPs for storing and processing purpose. However, outsourcing such data, which is often private or sensitive, into the clouds with no physical and limited digital control by the users raises serious security concerns to the data [2]. Furthermore, inappropriately handling such data could result in a disaster to the data owner due to data misuse, data leakage, or data stolen by other parties that use the same services. Moreover, the CSPs do not offer proper security guarantees to the data owners [3]. Due to the scale, dynamicity, openness and resource-sharing nature of cloud computing, addressing security issues in such environments is a very challenging problem [4]. 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. BACKGROUND OF THE WORK

### A - Mobile Cloud Computing

People would like to work and manage their daily life and tasks regardless of locations, times and situations. This requires the people to have mobile devices that can be carried everywhere at any time. Mobile devices have rapidly emerged and become popular with improved capabilities such as computing power, battery resources, security and privacy. As a result, the devices have been extended and improved to suit recent applications provided through the Internet like cloud computing. With such

improvements, people can accomplish their daily tasks like Internet banking, GPS, etc. conveniently and efficiently. Even though the capabilities on the mobile devices have improved, some applications demand extensive computing power and battery consumption. Wireless communication devices for instance appear to be highly power-consumptive. Several techniques in [5] have been introduced to reduce the power consumption and save the energy during the communication. Furthermore, the battery life can be extended by offloading large tasks for remote processing. Work in [5] shows that the portable computers executing their large tasks remotely can save up to 51% of battery power. Dinh, H., T., et al. [1] proposed a computation offloading technique with the objective to migrate large computations and complex processing from resource-limited devices like mobile devices to resourceful machines such as servers in clouds. This avoids taking a long application execution time on mobile devices, which would result in a large amount of power consumption. To apply this offloading technique, several works have been done to evaluate the effectiveness of such a technique through some experiments. The results demonstrate that the remote application execution can save energy significantly. On the other hand, storage capacity is also a constraint for mobile devices. Mobile cloud computing is developed to enable mobile users to store/access a large amount of data on the cloud through wireless networks. The Amazon Simple Storage is one of the examples that facilitate storage as a service. Another example is Image Exchange which utilizes the large storage space in clouds for mobile users. This mobile photo sharing service enables mobile users to upload images to the clouds immediately after capturing. Users may access all images from any devices. With the cloud, the users can save a considerable amount of energy and storage space on their mobile devices because all images are sent to, stored and processed on the clouds [1].

Moreover, in cloud computing, all services are delivered through web applications and data that has been outsourced is no longer owned by the users. Shifting all the data and computing resources to the cloud can have implications on privacy and security. Since the data is stored and managed on the cloud, security and privacy settings depend on the IT management provided by the cloud. The CSP typically works with many third-party vendors. There is no guarantee how these vendors may safeguard the data. Moreover, data on the cloud may be stored at multiple locations across different states and countries. Data that might be secure in one country may not be secure in another: different jurisdictions may apply over accessing the data. All these factors make it evident that all data cannot be stored in the cloud without considering the privacy and security implications. One possible solution to storing data is to encrypt the data before storage. This can prevent unauthorized access even when the storage is breached at the cloud. If the data is encrypted, then it has to be decrypted at the CSP because of the need to perform operations on the data. On the other hand, perform in encryption techniques before sending the data to the cloud requires some additional processing on the mobile system and consumes additional energy [6]. Furthermore, as mobile cloud computing is based on cloud computing, all the security issues are inherited in mobile cloud computing with the extra limitation of resource constraint mobile devices. Due to the resource limitation, the security algorithms proposed for the cloud computing environment may not work well directly on a mobile device. There is a need for a lightweight secure framework that provides security with 619 minimum communication and processing overhead on mobile devices [7].

**B - Security and Privacy in Mobile Cloud Computing**

Providing strong security and high privacy means requiring more computing resources and energy consumption Furthermore, increasing the security of data will decrease the functionality that can be executed on the data [8]. Therefore, a balance between security, functionality and energy consumption has to be the guideline in providing a scheme that can be implemented to the mobile data in an efficient manner. Due to this reason, a lot of research work has been conducted to provide security and improve privacy of outsourced data with consideration of the energy consumption and storage spaces. There are several approaches to securing the outsourced data using existing methods. The first approach is to ensure the integrity of users' data stored in cloud servers. Itani et al. [9] proposed an energy efficient framework for mobile devices to ensure the integrity of the mobile users' files/data stored on a cloud server using the concept of incremental cryptography and trusted computing. Furthermore, Jia et al. [10] introduced a secure data service that outsources data and security management to cloud in a trusted mode. The secure data services allow mobile users to outsource data and data sharing overhead to a cloud without disclosing any information about the shared data. To achieve the secure data service, the proxy re-encryption and identity-based encryption are implemented. The proposed secure data service provides not only data privacy but also fine-grained access control with the minimum cost of updating access policy and communication overheads. On the other hand, Shukla et al. [11] proposed a scheme for smart phones to ensure the security and integrity of mobile users' files stored on cloud servers. An archive mechanism that integrates cloud storage, hybrid cryptography, and digital signatures has been designed to provide security requirements for data storage of mobile phones. Such a mechanism not only can avoid malicious attackers from illegal access but also can share desired data and information with targeted friends by distinct access rights.

From our point of view, the schemes in [9] and [10] are based on the trusted mode. In mobile cloud environments, such schemes are not suitable for implementation as the cloud servers are assumed to be untrusted third parties. Therefore, they are not allowed to gain any information of the processed and stored data. Furthermore, work in [11] mainly focuses on security of the stored data. In mobile cloud environments, data storage is not the only services provided to the outsourced data. Data processing is one of the main services provided by the cloud servers as they have a huge amount of computing resources. Thus, securing the processed data is also important to prevent any security and privacy breaches to the user data. Based on such factors, LRE-MCDS is proposed to provide a security solution to the processed data. With an improved efficiency, the LRE-MCDS is believed to be the best scheme that enables data to be processed by third parties like cloud in an efficient and secure manner.

## III. OVERVIEW OF PROPOSED METHOD

The LRE-MCDS is proposed to enable mobile data to be outsourced and processed in cloud environments. However, data outsourcing itself is not the best approach to overcome the limitation of the mobile devices as the security and privacy of the data are highly important. Furthermore, heavy computation for securing the data on mobile devices before outsourcing degrades their battery lifetime. Thus, the security and computation complexity need to be balanced in order to provide a better scheme for the outsourcing data. According to this section, we describe the LRE-MCDS system design contributions.

The main contributions of LRE-MCDS are as follows:

1) An algorithm called LRE-MCDS based on Ciphertext Attribute-Based Encryption (CP-ABE) method to offer efficient access control over ciphertext.

2) Proxy servers for encryption and decryption operations. In this approach computational intensive operations in ABE are conducted on proxy servers, which greatly reduce the computational overhead on client-side mobile devices.

3) In LRE-MCDS of 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.

4) Introduce re-encryption, deduplication checking, fault recovery and description field of attributes to reduce the revocation overhead when dealing with the user revocation problem.

5)On the basis of algorithms we implement a data sharing prototype framework based on LRE-MCDS.

6) The experiments show that LRE-MCDS can greatly reduce the overhead on the client side, which only introduces a minimal additional cost on the server side.

7) An approach is beneficial to implement a realistic data sharing security scheme on mobile devices.

8) The results also show that LRE-MCDS has better performance compared to the existing ABE based access control schemes over ciphertext.

## IV. WORKING OVERVIEW

**LRE-MCDS, a framework of lightweight data-sharing scheme in mobile cloud. It has the following six components.**

- Data Client (DC): It is a third party organization that requires information from the data distributors in relation to specific tasks and purposes. It has low computing resources and storage spaces. It leverages the technology provided by the cloud to compute and store data purposely.
- Data Owner (DO): DO uploads data to the mobile cloud and share it with friends. DO determines the access control policies.
- Data User (DU): DU retrieves data from the mobile cloud.
- Trust Authority (TA): TA is responsible for generating and distributing attribute keys.
- Encryption Service Provider (ESP): ESP provides data encryption operations for DO.
- Decryption Service Provider (DSP): DSP provides data decryption operations for DU.
- Cloud Server (CS): A third party organization which possesses a huge amount of computing power and storage space for computing and storing purposes. It is an untrusted party. CS provides a lot of Internet based applications and delivers as a service to the client through Internet connection. The client just needs to pay on a per use basis without any hassle to manage the software license, maintenance, etc.

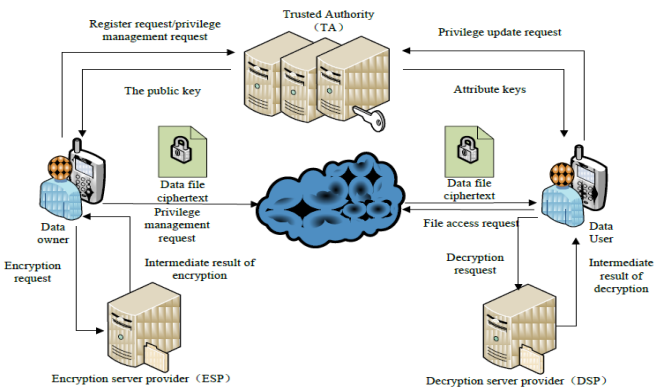


*Fig-1: Application design of LRE-MCDS*

To address privacy issue in existing system we propose a crypto-system for secure sharing of data over the cloud, which uses combination Attribute Based Encryption and Rivest Cipher 6 (RC-6) Algorithm for Re-encryption of data to securely transfer the data between the users.

Data Uploader/Owner: The Main Responsibility of the Data Uploader is to upload a data to the cloud storage and view the files what the different uploaders uploaded. To download that document uploader, have to get a key from the Authority.

Authority: The Authority people is able to view the list of data uploaders, users in this case he has another option if he need to add the data uploader. He need to add otherwise delete and also he is able to give the keys for the requests from the data user and data uploader.

Data User: The Data user can able to view the files if he wants to download the file he need to send the request to authority, after receiving the key he need to download.

## V. PROPOSED SYSTEM ENCRYPTION ALGORITHM

RC6 is a symmetric key block cipher derived from RC5, Block size of 128 bits, flexibility of key size, No key separation, Operators involved are simple in function favorably, High speed with minimal code memory. provides a solid well-tuned margin for security against well-known differential & linear attacks, Max potential for parallelism when multiple streams are processed.

Working – RC6

RC6 works with four w-bit Registers A; B; C; D which contain the initial input plain text as well as the output ciphertext at the end of encryption. The first byte of plain text or ciphertext is placed in the least-Signiant byte of A; The last byte of plaintext or ciphertext is placed in to the most-Signiant byte of D we use (A; B; C; D) = (B; C;D;A ) To mean the parallel assignment of values on the right to registers on the left.

## VI. CONCLUTION

In this paper, the issue of sharing the data in cloud computing securely is resolved. Data privacy can be maintained by combination of ABE and Rivest Cipher 6 (RC6) algorithm. Authentication is used to guarantee data privacy and data integrity. This indicates that the proposed system can be used to enhance privacy preservation in cloud services.In future work, we will design the new approaches to ensure data integrity. To further tap the potential of mobile cloud, and also ensure how to do cipher text retrieval over existing data sharing schemes.

## REFERENCES

[1] H. T. Dinh, C. Lee, D. Niyato, and P. Wang, “A Survey of Mobile Cloud Computing: Architecture, Applications, and Approaches,” Wireless Communications and Mobile Computing, no. 13, pp. 1587– 1611, 2013.
[2] S. Singh and I. Chana, “Cloud Based Development Issues: A Methodical Analysis,” International Journal of Cloud Computing and Services Science, vol. 2, no. 1, pp. 73–84, 2013.
[3] K. Nahrstedt, R. Campbell, E. Burger, J. Giffin, X. H. Gu, A. D. Joseph, E. Keller, D. Ma, and H. Weatherspoon, “Security for Cloud Computing,” in A Report: Directorate for Computer and Information Science and Engineering (CISE), pp. 1–19, 2012.
[4] D. Zissis and D. Lekkas, “Addressing cloud computing security issues,” Future Generation Computer Systems, vol. 28, no. 3, pp. 583– 592, Mar. 2012.
[5] R. P. Rudenko A., “Saving Portable Computer Battery Power through Remote Process Execution,” Mobile Computing and Communication Review, vol. 2, no I, pp. 19–26, 1998.
[6] K. Kumar and Y.-H. Lu, “Cloud Computing for Mobile Users: Can Offloading Save Energy?,” IEEE Computer, pp. 51–56, 2010.
[7] A. N. Khan, M. L. Mat Kiah, S. U. Khan, and S. a. Madani, “Towards secure mobile cloud computing: A survey,” Future Generation Computer System, vol. 29, no. 5, pp. 1278–1299, 2012.
[8] A. Boldyreva, G. Tech, P. Grubbs, and S. Networks, “Making encryption work in the cloud,” Network Security, vol. 2014, no. 10, pp. 8–10, 2014.
[9] W. Itani, A. Kayssi, and A. Chehab, “Energy-efficient incremental integrity for securing storage in mobile cloud computing,” 2010 International Conference on Energy Aware Computing, ICEAC 2010, pp. 26–27, 2010.
[10] W. Jia, H. Zhu, Z. Cao, L. Wei, and X. Lin, “SDSM : A Secure Data Service Mechanism in Mobile Cloud Computing,” The First International Workshop on Security in Computers, Networking and Communications, pp. 1060–1065, 2011.
[11] S. C. Hsueh, J. Y. Lin, and M. Y. Lin, “Secure cloud storage for convenient data archive of smart phones,” Proceedings of the International Symposium on Consumer Electronics, ISCE, vol. 18, no. 51, pp. 156–161, 2011.