Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 6.017

IJCSMC, Vol. 7, Issue. 12, December 2018, pg.328 – 332

Novel Secure Lightweight Data Sharing Framework for Mobile Cloud Computing

K.Mehala M.Sc, B.Ed**, Dr. A.Senthil Kumar** M.Sc, Mphill, Phd

Mphill-Computer Science & Tamil University Thanjavur, India

Mphill-Computer Science & Tamil University Thanjavur, India

Mehalamurali2005@gmail.com; erodesenthilkumar@gmail.com

Abstract— With the innovations of cloud computing, mobile devices can store/retrieve data and protected information from anywhere at any time. On the other hand, information security is the main concern in mobile cloud computing. There are various studies that have been conducted to progress the mobile cloud security. However, most of the proposed methods are not appropriate for mobile cloud because of limited computing resources and power. Solutions with low computational overhead are in great necessity for mobile cloud applications. In this project, we suggest a Novel Secure Lightweight Data Sharing Framework for Mobile Cloud Computing for mobile cloud computing. It based on CP-ABE (Cipher Policy-Attribute Based Encryption) an access control technology used in a normal cloud environment but modifies the structure of access control tree to make it fit for mobile cloud environments. In this project, we improve the processing speed and performance of the mobile cloud we have added an external proxy server. The results evaluation shows that the proposed system efficiently improves the processing speed and provides high security.

Keywords— Mobile Cloud Computing, Cloud Computing, security, access control, user revocation, cryptography

I. INTRODUCTION

Rapid development of cloud computing[6] and the reputation of smart phones are progressively getting adapted 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. However, smartphones have restricted processing power and storage space whereas the cloud provide numerous options to store and process the data. Nowadays, different kinds of mobile applications have been usually used. In this application, anyone can easily upload and share their photos, videos, documents and other protected information with other people. However, data security is the major concern for this method adversary can easily hack our secret information. To address this problem, in this research, we propose a Novel Secure Lightweight Data Sharing Framework for Mobile Cloud Computing

environment. The main contributions of SDSS are as follows. We proposed an algorithm called SLDS-CP-ABE based on Attribute-Based Encryption (ABE) method to deliver efficient access control and security over cypher text. Introduce proxy servers for both encryption and decryption. In this system processing overhead rapidly reduced. Finally, we implement as data sharing prototype framework based on SLDS-CP-ABE.

1.1 Attribute-based encryption

Attribute-based encryption[5] is public-key encryption, which the secret key of a user and the ciphertext are dependent upon attributes e.g., roles, and messages can be encrypted with respect to subsets of attributes (key-policy ABE - KP-ABE). Attribute-based encryption is shared into two categories: First the Ciphertext-Policy Attribute Based Encryption (CP-ABE) where the access control policy is embedded into ciphertext; the other one is Key-Policy Attribute Based Encryption (KP-ABE) where the access control policy is embedded in the user's key attributes. In real applications, CP-ABE is more appropriate since it look like role-based access control. In CP-ABE, the data owner proposal the access control policy and allocates attributes to data users. A user can decrypt the data properly when the user's attributes fulfil the access control policy.

1.2 Trusted Authority

In this research, to make SLDS-CP-ABE realistic in practice, a trusted authority (TA) is introduced. It is accountable of generating public and private keys, and distributing attribute keys to users. With this systems, users can share and access data without being aware of the encryption and decryption operations. We assume TA is totally credible, and a trusted channel exists between the TA and every user. As the trusted channel exists it doesn't mean that the data can be shared through the trusted channel, for the data can be in a large amount. TA is only used to transfer keys (in a small amount) steadily between users. Further it's requested that TA is online all the time because data users may access data at any time and need TA to update attribute keys.

II. LITERATURE REVIEW

[1]Yu Jin, Chuan Tian, Heng He and Fan Wang presented a secure and lightweight data access control scheme named SL-CP-ABE. The proposed method can preserve the privacy of outsourced data and achieve fine-grained data access control efficiently in MCC. This method enhance the overall system performance by reducing the computation overheads in encryption and decryption operations, provide flexible and expressive data access control policy, and allow data owners to securely outsource the computation overheads at mobile devices to cloud servers.

Chenglin Shen and Heng He proposed A Lightweight Secure Data Sharing Scheme for Mobile Cloud Computing. [2], Design LDSS-CP-ABE algorithm for providing security to the mobile cloud computing. This method describes that Mobile device has limited computing resources and limited storage and so data can be stored on cloud computing. According to [2] any user can upload their data on mobile cloud and moreover anyone can access to that data. Based on this method there is security concern related to that uploaded data, LDSS-CP-ABE should provide security to that uploaded data to prevent it from adversary.

[3]Piotr K. Tysowski and M. Anwarul Hasan introduced Hybrid Attribute- and Re-Encryption-Based Key Management for Secure and Scalable Mobile Applications in Clouds. They developed a protocol for outsourcing data storage to a cloud service provider for improving data security. In addition, improving the performance of attribute based encryption and additional security are provided through a group keying mechanism. In this paper, re-encryption mechanism is performed optionally.

[4]Xiuxia Tian and Xiaoling Wang developed DSP RE-Encryption: A Flexible Mechanism for Access Control Enforcement Management in DaaS. In this method, they have introduced an approach to implement the flexible access control enforcement management by applying a DSP re-encryption mechanism. In addition the proposed method satisfies the secure performance of the confidentiality and can reduce the computation overhead of the client by eliminating the public catalog of tokens.

III.PROPOSED METHODOLOGY

When we analyse the literature survey it is found that many different types of framework for the mobile cloud have been implemented. Still, there are the security issues and data sharing issues. In order to overcome the security issues and data sharing issues we should implement a robust secure light weight data sharing method for mobile cloud computing. Fig 1 shows the architecture of the proposed method.

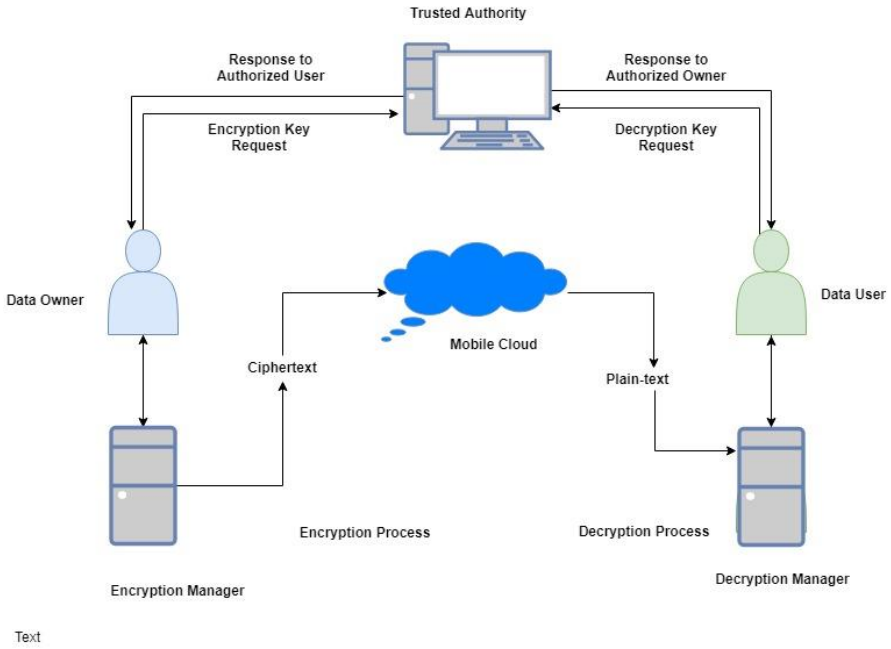

Fig. 1 Secure Lightweight Data Sharing Framework for Mobile Cloud Computing.

There are six important modules in the work we have proposed. They are Data Owner (DO), Data User (DU), Trusted Authority (TA), Encryption Manager, Decryption Manager and Cloud Service Provider. Of these, the chief work of the Trusted Authority is to generate encryption key for the DO and decryption key for Du. The DO is the owner of the data to be encrypted. The DO gets the encryption key from the TA. The data to be encrypted is based on the attribute. DO first encrypts the data and then shares the ciphertext on the mobile cloud. The authorized DU gets the decryption key from the TA. The decryption manager is used to decrypt the data for authorized DU. In the encryption and the decryption processes we use a proxy server to make the encryption and the decryption processes lightweight. Finally it is the cloud service provider which manages all this system.

IV. EXPERIMENTAL ANALYSIS

In order to implement this proposed work we have used J2EE, MySql and DriveHQ. In this proposed work there is separate authentication (login) page for DO, DU, TA and CSP. Fig 2 shows the DU login screen. The CSP provides access permission to DO, DU and TA. As soon as the access permission is obtained the DO can upload the ciphertext on the mobile cloud. In addition, the authenticated user can view the uploaded file into plaintext format. The TA provides the key management process to the DO and the DU. Fig 3 shows the key request screen. Fig 4 shows the ciphertext. Our proposed experimental result shows that Novel Secure Lightweight Data Sharing Framework for Mobile Cloud Computing provides high security over the previous works.

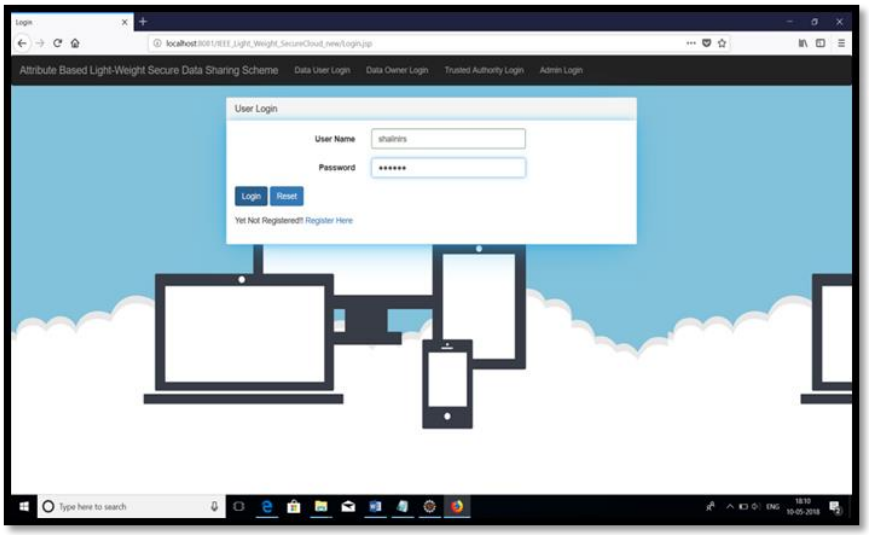

Fig 2 DU login screen

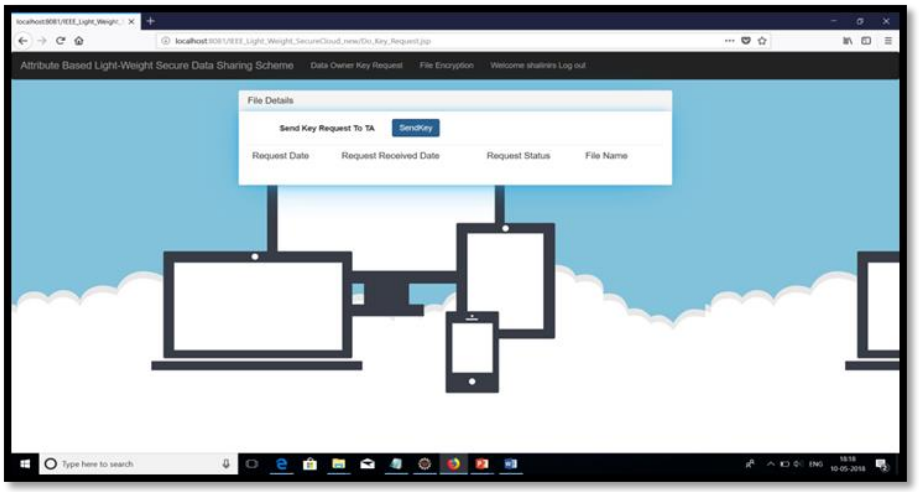

Fig 3 DO key requst to TA

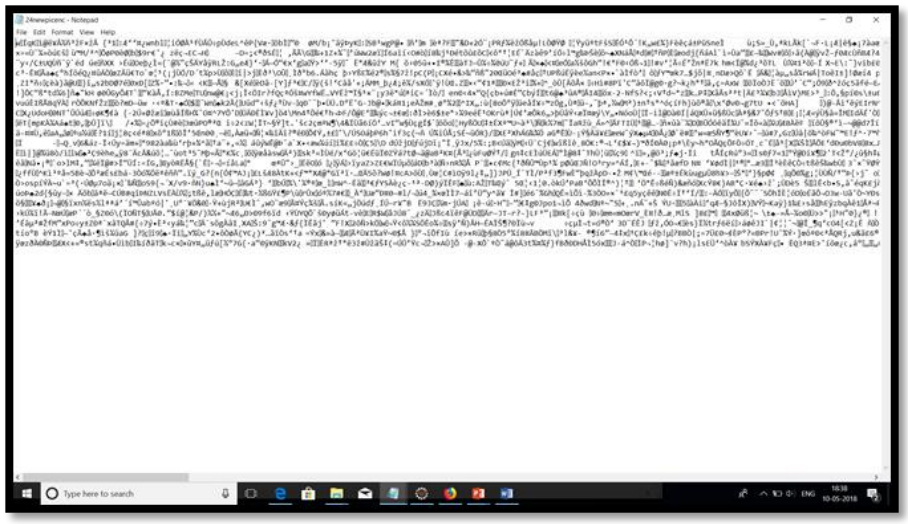

Fig 4 chipertex

V. CONCLUSIONS

In this research first we discussed on the security concern and the difficulty in the data sharing. For solving this difficulty we have implemented a proposed method which is lightweight and secure. This will improve the security of data and enhance the speed of the mobile cloud many times. Comparing with the pervious works there is significant advance in our proposed work. Firstly, the performance of the proposed work is improved much and the encryption and the decryption parts are made lightweight. As the attribute based encryption is used the security is improved multiply. On the future work are to develop an approach that would maintain data integrity.

REFERENCES

[1] Yu Jin ; Chuan Tian ; Heng He ; Fan Wang, "A Secure and Lightweight Data Access Control Scheme for Mobile Cloud Computing", 2015 IEEE Fifth International Conference on Big Data and Cloud Computing.

[2] Chenglin Shen, Heng He, "A Lightweight Secure Data Sharing Scheme for Mobile Cloud Computing", IEEE TRANSACTIONS ON CLOUD COMPUTING, 2014.

[3] Piotr K. Tysowski, M. Anwarul Hasan, "Hybrid Attribute- and Re-Encryption-Based Key Management for Secure and Scalable Mobile Applications in Clouds" IEEE Transactions on Cloud Computing., vol. 2, 2013.

[4] XiuXia Tian, XiaoLing Wang, AoYing Zhou, "DSP RE-Encryption: A Flexible Mechanism for Access Control Enforcement Management in DaaS," IEEE 2009 IEEE International Conference on Cloud Computing.
[5] [Online]. Available: https://en.wikipedia.org/wiki/Attribute-based_encryption.
[6] [Online]. Availablehttps://en.wikipedia.org/wiki/Mobile_cloud_computing.

