International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 11 | Nov 2018 www.irjet.net p-ISSN: 2395-0072

# A Review on Lightweight Secure Data Sharing Scheme for Mobile Cloud Computing

**Heena Kausar Sharpyade[1], Mujamil Dakhani[2], SaimaRafat Bhandari[3]**

*[1,3]Student, Dept. of Computer Science and Engineering, Karnataka, India*
*[2]Asst. Professor, Dept. of Computer Science and Engineering, Karnataka, India*

---

**Abstract -** *As the increasing usage of the cloud computing has even mobile devices a new scope to retrieve and store the personal data from anywhere at any time. Due to increases in the data it has caused the data security problem over the mobile computing. There are lots of studies that have used to secure the cloud but most of them have the limitation for the mobile devices. The solution should be provided with the lower computational overhead. In this paper, the review on lightweight secure data sharing scheme (LDSS) for mobile cloud computing. For providing the satisfactory performance, it is important to use the resources provided by the cloud service provider (CSP) to store and share the data.*

***Key Words***: Cloud computing, Data Security, LDSS, CSP.

## 1. INTRODUCTION

With increasing of the cloud storage and more usage of mobile has increased the data sharing model which have been used for the data retroviral and storage. As the usage of cloud have been increased widely, due to limitation of mobile storage. The cloud have more amount of storage and resources which is provide by the cloud service provider to store and share the data. The cloud mobile applications such as upload of photos, videos, documents and other files to the cloud and these files can be used to share with other users. Management functionality is also provided by the cloud service provider, but the personal information is important and it should be not shared in publically. It is important to provide the data privacy and the data security which is the major concern. The control mechanism provided by the cloud service provider is not sufficient as it does not meet the requirement of the data owner, the first and far most problem is whenever the user uploads the files on cloud then the cloud service provider may spy on the file for its use which cause the privacy problem later the user want to send the password for the encrypted files to unlock it. To overcome these problem data owner have to divide the data user into different user according to the user who want to share their password to the particular group. Password management is a great issue for the security.

## 2. PROBLEM DEFINITION

### 2.1 Problem Statement

- To provide security in lightweight manner resource mobile devices in cloud environment
- To have light weight revocation policy.
- The encrypted and decrypted data should be secure using secret key.
- The sharing of the file should be among the authorized users who have the access privileges.
- There should also have the opportunity to decrease the overhead of the cryptographic standard algorithm and research the security schemes with low over head.

### 2.2 Proposed System

The proposed system is a Lightweight Data Sharing Scheme (LDSS) for mobile cloud computing environment. The main contributions of LDSS are as follows:

- It uses the designed algorithm called LDSS-CP-ABE based Attribute-based Encryption (AES) used for access control over ciphertext efficiently.
- Here the proxy servers are used for encryption and decryption methods. ABE is used for the computational intensive operations for conducting on the proxy servers, which help in reducing the computational overhead on the client side of the mobile devices. There is also maintaining of the data privacy using LDSS-CP-ABE. The modified version of decryption key is sent in secure manner to the proxy servers.
- To deal with user's revocation problem the lazy re-encryption and decryption field of attributes are introduced
- Lastly, to have a data sharing framework prototype based on LDSS.

**Advantages of proposed system**:

- LDSS has reduces the over head at the client side due which it has reduce the additional cost at the server side.
- These approaches have increased the security of the data sharing on mobile devices.
- LDSS has the better performances results based on access control schemes over ciphertext compared to exiting ABE.
- The overhead is reduced when the multiple revocation operations are merged as one.
- The data storage overhead is small.

## 3. LITERATURE SURVEY

To study and analyze more about lightweight secure data sharing scheme (LDSS) for mobile cloud computing, the following literature survey has been done.

In [1] the author present an efficient fully homomorphic encryption scheme that is based on the standard learning with errors (LWE) assumption. By applying the results which are been known on learning with errors, here the worst case been used for the security hardness problems of the short vector. Here the improvement is done on the previous works on two aspects firstly the previous complexity assumption scheme related to deals in various rings are replaced by the homomorphic encryption based on learning with error using a new re- linearization technique. And secondly the squashing paradigm is introduced based on previous works. There is also new dimension modulus reduction technique to reduces decryption complexity.

In [2] authors presents the data leakage mitigation for discretionary access control in collaboration cloud. The systems to Software as a Service (SaaS) applications is been collaborated as the usage of the cloud computing has increased. SaaS collaboration has more number of advantages but it has some security issues. As the SaaS collaboration is increased there is chance of leakage of the information while sharing to the intruders. There is proposing to mitigate the data leakage problem in SaaS collaboration systems by reducing human errors. There can be series of mechanism to reduces the leakage of the data by allowing the entropies to encodes their organisational security rules mandatory to access the sharing decisions, by prioritizing the potential recipients of the users files to reduces the error and to examines the abnormal recipients.

In [3] the authors speak about the implementing deniable storage encryption for mobile devices. Data confidentiality is the one of the most important accept and it can use by encryption. As providing encryption will cover the user information and by using the keys. The data is been hidden so that it cannot be read by the intruders. To solve specific problems, by using Steganographic techniques and deniable encryption algorithms. After evaluating existing and discover new, there are some challenges that are comprised plausibly deniable encryption (PDE) in mobile environment. To solve these problems a new system is been designed called Mobiflage that enables PDE on mobile devices for hiding encrypted volumes for the external storage.

In [4] authors present a secure and efficient access to outsourced data in. The main aspect is to provide security and efficient access to large scale outsourced data. Here the new mechanism to solve the problem of owner-write-users-read application is introduced. To efficiently achieve the flexible cryptography based access control is done by using encryption to every block of data by using different keys. But to use the key derivation methods the owner needs to have some secrets. Using hash functions for analysis key derivation will reduces the computational overhead. And also getting the access to updated data blocks can be done by using over encryption and/or lazy revocation.

In [5] the authors present the attribute base fine grained access control with efficient revocation in cloud storage system. Here the users are allowed to store the data to the cloud and also provides for data to be used in the cloud storage. As the cloud server and the data owners are not in the same trust domain, so there cannot be semi trusted cloud server to rely on the access policy. To solve the challenges, traditional methods are been used where the data is been encrypted and send with the decryption keys to authorised users. This traditional method has the high overhead and complicated key management. To overcome these challenges a new design is used to access control framework for the cloud storage systems by Ciphertext-policy Attribute- based Encryption(CP-ABE) approach.

## 4. METHODOLOGY

The LDSS framework for lightweight data sharing scheme in mobile cloud is shown in Fig. 4.1. It has the following three components:

- Data Owner (DO): Data Owner is used to upload the data to the mobile cloud and share it with other users. DO determine the access control policies.
- Data User (DU): Data User is used to retrieves data from the mobile cloud.
- Trust Authority (TA): Trust Authority is responsible for generating and distributing attribute keys.

As shown in Fig. 4.1, a Data Owner sends data to the cloud. Since the cloud is not trustworthy, so data has to be encrypted before it is uploaded. The Data Owner access the control tree on the data files to assign which attributes a data user to obtain the certain data files though access control policy. The data files in the LDSS are encrypted in the symmetric order and the symmetric keys of the data encryption is done using Attribute Based Encryption(ABE). The symmetric key, access control policy is embedded with ciphertext. The data user who has authority can access control policy which is encrypted these can be decrypted and the symmetric key can be retrieve.

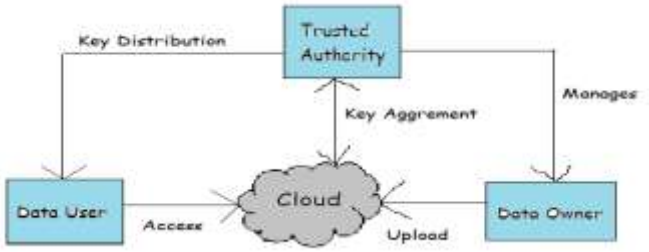


**Fig -4.1**: A lightweight data-sharing scheme (LDSS) framework

## 5. RESULT AND CONCLUSIONS

It uses the LDSS which provide the data privacy in the mobile cloud and also reduces the overhead of mobile cloud on user's side. It has the login page for the data user, data owner and the trust authority as shown in Fig 2. There are the registration forms for the data owner and the data user as shown in Fig 3. There is home page for data user, data owner and trust authority as shown in Fig 4. Depending on particular user the following page pop up as shown in Fig 5.

In data owner the file is uploaded and sends for the encryption as shown in Fig 6 and 7. Then it is send to the cloud for upload of the file as shown in Fig 8. Later the uploaded files can be seen in the data owner page as shown in Fig 9. On clicking view cloud files and verifies attributes in data user page as shown in Fig 10. Then on clicking on decryption as shown in Fig 11, the file can be downloaded as shown in Fig 12. Verify user attributes is checked on trust authority page as shown in Fig 13. The view owner in trust authority page is shown in the Fig 14.

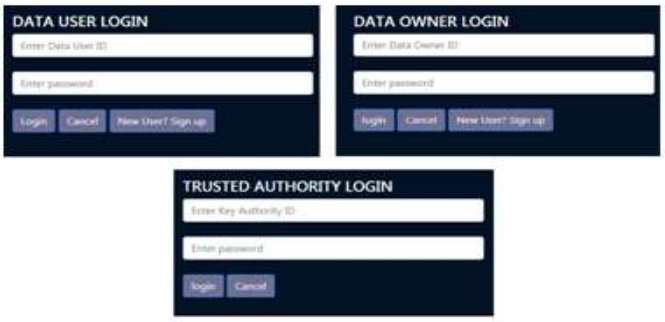


**Fig -2**: Login page for Data User, Data Owner and Trust Authority

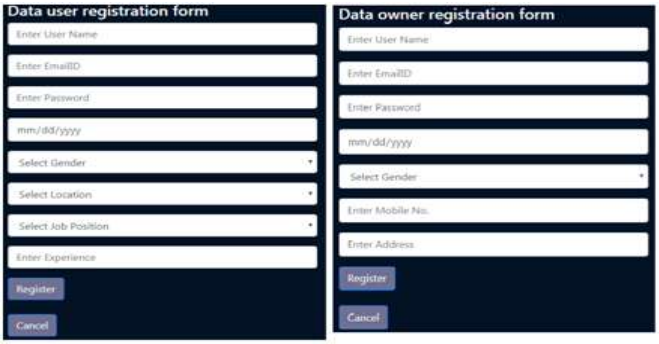


**Fig -3**: Signup Page for data user and data owner

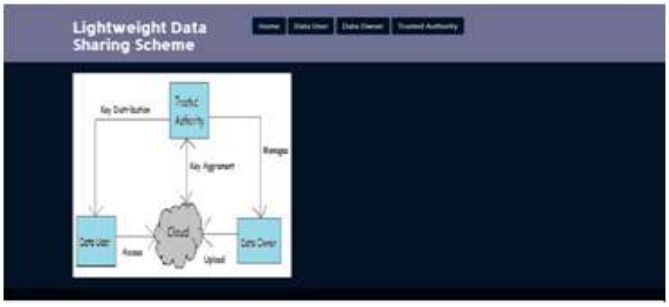


**Fig -4**: Home page


**Fig -5**: File uploads in Data owner


**Fig -6**: After clicking on send files for encryption in data owner page


**Fig -7**: After Clicking on upload files to Cloud in data owner page


**Fig -8**: After clicking on uploaded files in data owner page

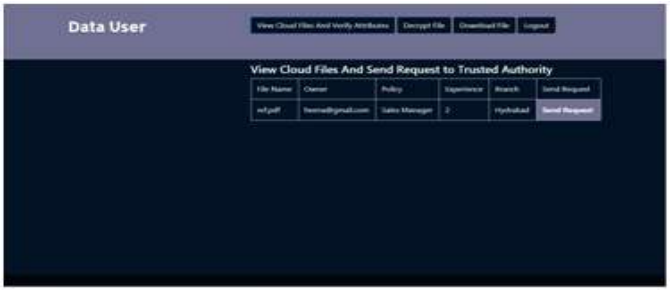


**Fig -9**: After clicking on view cloud files and verify attributes in data user page


**Fig -10**: After clicking on decrypt file in data user page


**Fig -11**: Once we click decrypt file button from the list in data user page


**Fig -12**: Clicking on download link in data user page


**Fig -13**: After clicking on verify user attributes in trust authority page

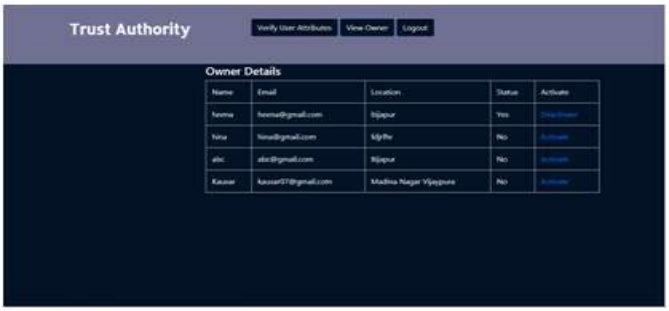


**Fig -14**: After clicking on view owner in trust authority page

## REFERENCES

[1] 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.

[2] 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.

[3] 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.

[4] 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.

[5] Junzuo Lai, Robert H. Deng ,Yingjiu Li ,et al. Fully secure key-policy attribute-based encryption with constant-size ciphertexts and fast decryption. In: Proceedings of the 9th ACM symposium on Information, Computer and Communications Security (ASIACCS), pp. 239-248, Jun. 2014.

[6] 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.

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

[8] Benjamin Livshits, Jaeyeon Jung. Automatic Mediation of Privacy-Sensitive Resource Access in Smartphone Applications. USENIX Security, pp.113-130, Aug. 2013.

[9] Kan Yang, Xiaohua Jia, Kui Ren, Bo Zhang, Ruitao Xie: DAC-MACS: Effective Data Access Control for Multiauthority Cloud Storage Systems. IEEE Transactions on Information Forensics and Security, Vol. 8, No. 11, pp.1790-1801, 2013.