A Lightweight Secure Data Sharing Scheme for Mobile Cloud Computing

K.Naveena[1], S.Kusma[2]
[1] *Student, Dept. of MCA, EAIMS*
[2] *Professor, Dept. of MCA, EAIMS, Tirupati, A.P.*

***Abstract*- With the popularity of cloud computing, mobile devices can store and retrieve personal information from anywhere at any time. Consequently, the data security problem in mobile cloud becomes more severe and prevents further development of mobile cloud. There are substantial studies have been conducted to improve the cloud security. Most of them are not applicable for mobile cloud since mobile devices has limited computing resources and power. Solutions with low computational overhead are in great need for mobile computing cloud applications. In this paper, we propose a lightweight data sharing scheme (LDSS) for mobile cloud computing. Cloud has been around for two decades and it consists of the vast amount of data from all over the world. Most of the people at a personal level and organization level have moved their data to the cloud and share data across all-around the world. The main challenge faced by everyone is to share the data all over the world or at organizational level securely without giving away the important data to any exploiters. To overcome the challenge to share the data securely over the cloud, an efficient data encryption algorithm for encrypting data before sending it to the cloud. In this proposed we are using a combination of Attribute-BasedEncryption and Byte Rotation Encryption 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.**

INTRODUCTION

With the improvement of cloud computing the popularity of smart mobile devices, people are gradually getting into 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. Typically, mobile devices only have limited storage space and computing power. On the contrary, the cloud has enormous amount of resources. In such a scenario, to achieve the satisfactory performance, it is essential to use the resources provided by the cloud service provider (CSP) to store and share the data. 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.

EXISTING SYSTEM

With the continuous growth in development of cloud computing people are getting adept and accustomed 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. Typically, mobile devices only have limited storage space and computing power. On the contrary, the cloud has

enormous amount of resources. In such a scenario, to achieve the satisfactory performance, it is essential to use the resources provided by the cloud service provider to store and share the data.The development of cloud computing and the popularity of smart mobile devices, people are gradually getting accustomed 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. Typically, mobile devices only have limited storage space and computing power. On the contrary, the cloud has enormous amount of resources. In such a scenario, to achieve the satisfactory performance, it is essential to use the resources provided by the cloud service provider to store and share the data.

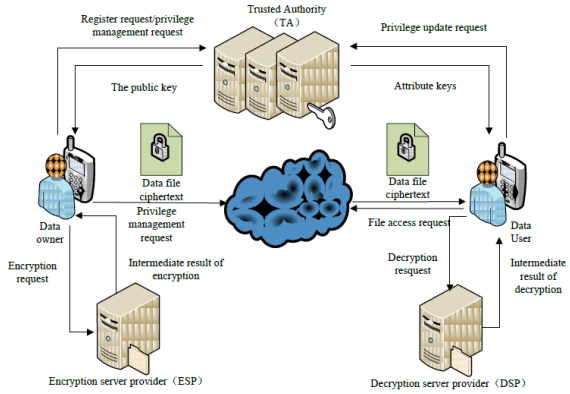
Disadvantages:

1. There is no proper mechanism to provide the security for the data presented in the mobile cloud.
2. User authentication and revocation cost will be high.

PROPOSED SYSTEM

The architecture of the proposed system is shown in the figure which shows the users and the operations involved. The detailed description of the architecture is explained as follows: • Nodes: The User is responsible for uploading and sharing its personal data on the cloud. • On-line and Off-line Services: In On-line Service data will encrypted and directly transfer to the respective user. In Off-line Service if there is no Internet Connection the data will get encrypted first and then it will get stored in Main Server. Until the system does not comes on-line the data will not be shared over the cloud • Cloud Service Provider: Cloud service provider is responsible for providing all the required services to its users according to their demands. • Encryption and Decryption: Here we are using the combination of ABE and BRE algorithm to encrypt and decrypt the files. • File Upload and Download: The file which are uploaded on cloud are encrypted form. Users

ARCHITECTURE DIAGRAM



Application design

Uploader:

The Main Responsibility of the Uploader is To upload a Document 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 uploader, users in this case he has the another option if he need to add the uploader he need to add otherwise delete and also he is able to give the keys for the requests from the user and uploader.

User:

The 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.

MODULES

1. Owner
2. Authority
3. User

Owner:

The Main Responsibility of the owner is to upload a Document to the cloud storage. And view the files what the different owner uploaded. To download that document owner have to get a key from the Authority.

Authority:

The Authority people is able to view the list of owner, users in this case he has the another option if he need to add the owner he need to add otherwise

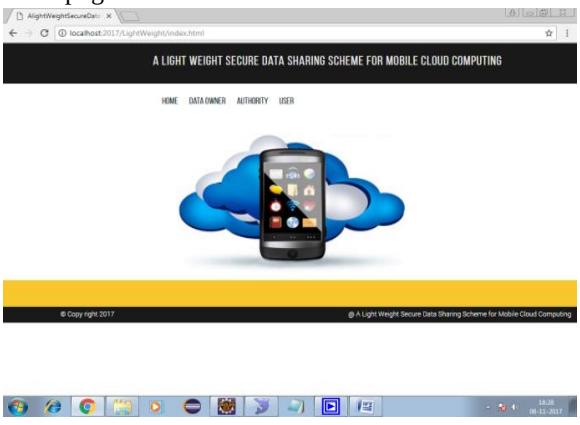
delete and also he is able to give the keys for the requests from the user and owner.

User:

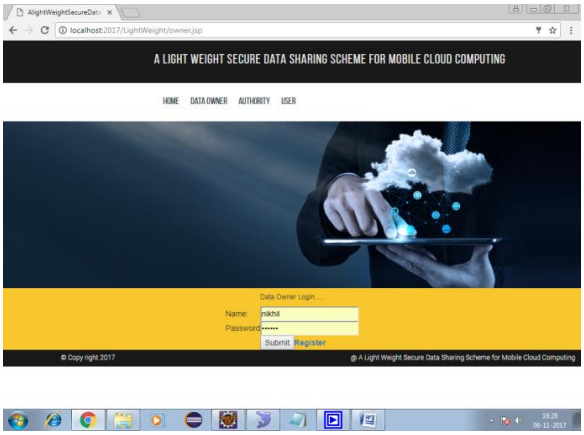
The user can able to view the files if he wants to download the file he need to send the request to Authority after receiving the key he need to download.

FINAL OUTPUT

Homepage:



Data Owner



Login:

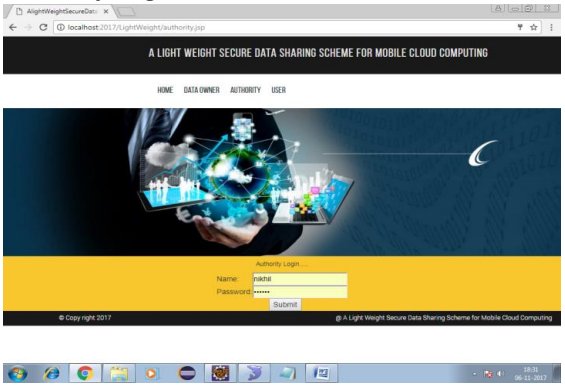
Data owner Home:

Upload File:

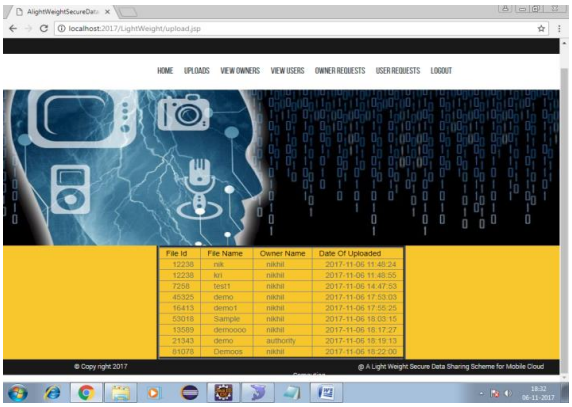
View files:

Download

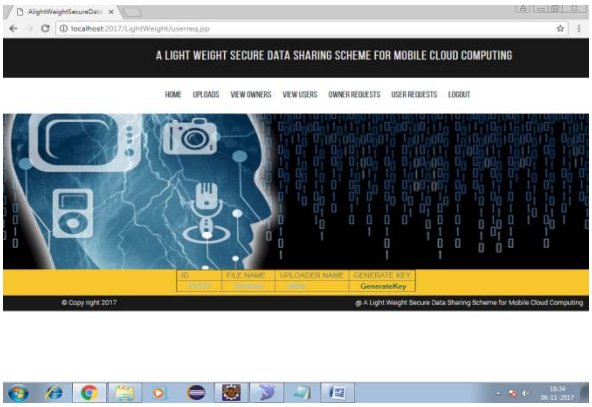
Authority Login:` ``



Uploads:

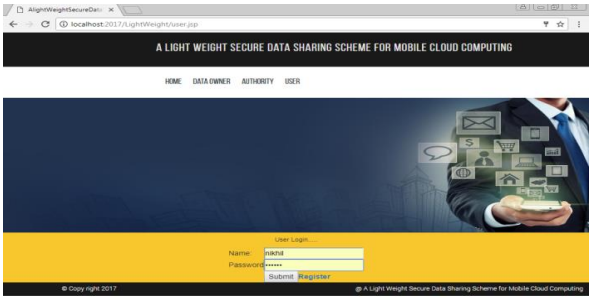


User Requests:



View Owners:

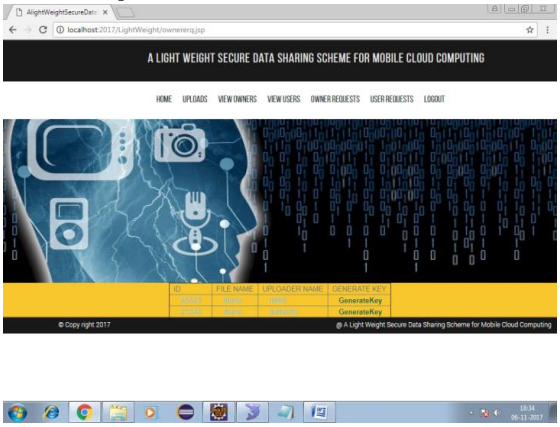
User Login:



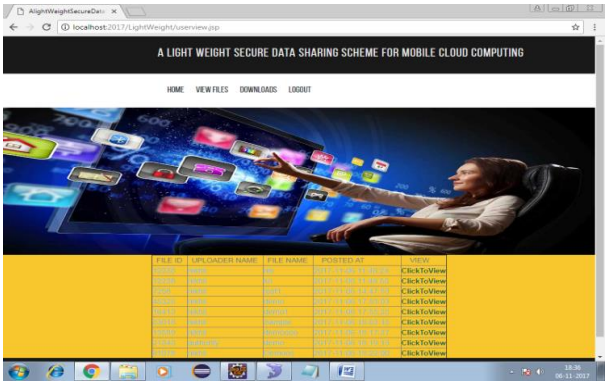
View Users:

User Home:

Owner Requests:



View Files:



Downloads:

CONCLUSION

In recent years, many studies on access control in cloud are totally based on attribute-based encryption algorithm (ABE). However, traditional ABE is not suitable for mobile cloud because it is computationally intensive and mobile devices has limited resources. In this paper, we propose LDSS to address this issue. It introduces a novel LDSS-CP-ABE algorithm to migrate major computation overhead from mobile devices onto proxy servers, thus it can help in solving the secure data sharing problem in mobile cloud. The experimental results show states that LDSS can ensures data privacy in mobile cloud and reduce the overload on users' side in mobile cloud. 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] Gentry C, Halevi S. Implementing gentry's fully-homomorphic encryption scheme. in: Advances in Cryptology–EUROCRYPT 2011. Berlin, Heidelberg.

[2] Brakerski Z, Vaikuntanathan V. Efficient fully homomorphic encryption from (standard) LWE. in: Proceeding of IEEE Symposium on Foundations of Computer Science. California, USA.

[3] Qihua Wang, Hongxia Jin. "Data leakage mitigation for discertionary access control in collaboration clouds". the 16th ACM Symposium on Access Control Models and Technologies.

[4] Adam Skillen and Mohammad Mannan. On Implementing Deniable Storage Encryption for Mobile Devices. the 20th Annual Network and Distributed System Security Symposium .

[5] 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.

[6] Maheshwari U, Vingralek R, Shapiro W. How to build a trusted database system on untrusted storage. in: Proceedings of the 4th conference on Symposium on Operating System Design & Implementation.

[7] Kan Yang, Xiaohua Jia, Kui Ren: Attribute-based fine-grained access control with efficient revocation in cloud storage systems.

[8] Crampton J, Martin K, Wild P. On key assignment for hierarchical access control. in: Computer Security Foundations Workshop.

[9] Shi E, Bethencourt J, Chan T H H, et al. Multi-dimensional range query over encrypted data. in: Proceedings of Symposium on Security and Privacy (SP).

[10] Cong Wang, Kui Ren, Shucheng Yu, and Karthik Mahendra Raje Urs. Achieving Usable and Privacy-assured Similarity Search over Outsourced Cloud Data.

[11] Yu S., Wang C., Ren K., Lou W. Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing.

[12] 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.

[13] Stehlé D, Steinfeld R. Faster fully homomorphic encryption. in: Proceedings of 16th International Conference on the Theory and Application of Cryptology and Information Security. Singapore.

[14] 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).

[15] Bethencourt J, Sahai A, Waters B. Ciphertext-policy attribute based encryption. in:

Proceedings of the 2007 IEEE Symposium on Security and Privacy (SP). Washington, USA: IEEE Computer Society.

[16] 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.

[17] 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.

[18] Yu S., Wang C., Ren K., et al. Attribute based data sharing with attribute revocation. in: Proceedings of the 5th International Symposium on Information, Computer and Communications Security (ASIACCS), New York, USA.

[19] Sandhu R S, Coyne E J, Feinstein H L, et al. Role-based access control models. Computer.

[20] Tian X X, Wang X L, Zhou A Y. DSP RE-Encryption: A flexible mechanism for access control enforcement management in DaaS. in: Proceedings of IEEE International Conference on Cloud Computing.

[21] 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.