
A LIGHT WEIGHT SECURE DATA SHARING SCHEME FOR MOBILE COLUD COMPUTING

K. Rambabu¹, B. Gnaneswara Rao,

¹Assistant professor(HOD) , PG DEPT, Dantuluri Narayana Raju College, **Bhimavaram, Andharapradesh**
Email:- kattarambabudnr@gmail.com

²PG Student of M.Sc, Dantuluri Narayana Raju College, **Bhimavaram, Andharapradesh**
Email:- ballagnaneswar33@gmail.com

ABSTRACT

With the popularity of cloud computing, mobile devices can store/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 lightweight data sharing scheme (LDSS) for mobile cloud computing. 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. LDSS 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 LDSS can effectively reduce the overhead on the mobile device side when users are sharing data in mobile cloud environments.

1 INTRODUCTION

What is cloud computing?

Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet). The name comes from the common use of a cloud-shaped symbol as an abstraction for the complex infrastructure it contains in system diagrams. Cloud computing entrusts remote services with a user's data, software and computation. Cloud computing consists of hardware and software resources made available on the Internet as managed third-party services. These services typically provide access to advanced software applications and high-end networks of server computers.

Literature Survey

Attribute-based fine-grained access control with efficient revocation in cloud storage systems

AUTHORS: Kan Yang, Xiaohua Jia, Kui Ren

A cloud storage service allows data owner to outsource their data to the cloud and through which provide the data access to the users. Because the cloud server and the data owner are not in the same trust domain, the semi-trusted cloud server cannot be relied to enforce the access policy. To address this challenge, traditional methods usually require the data owner to encrypt the data and deliver decryption keys to authorized users. These methods, however, normally involve complicated key management and high overhead on data owner. In this paper, we design an access control framework for cloud storage systems that achieves fine-grained access control based on an adapted Ciphertext-Policy Attribute-based Encryption (CP-ABE) approach. In the proposed scheme, an efficient attribute revocation method is proposed to cope with the dynamic changes of users' access privileges in large-scale systems. The analysis shows that the proposed access control scheme is provably secure in the random oracle model and efficient to be applied into practice.

3 IMPLEMENTATION STUDY

EXISTING SYSTEM:

In general, we can divide these approaches into four categories: simple ciphertext access control, hierarchical access control, access control based on fully homomorphic encryption and access control based on attribute-based encryption (ABE). All these proposals are designed for non-mobile cloud environment

Disadvantages:

- 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.

Proposed System & algorithm

- We propose a Lightweight Data Sharing Scheme (LDSS) for mobile cloud computing environment.

4.1 Advantages:

- 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.

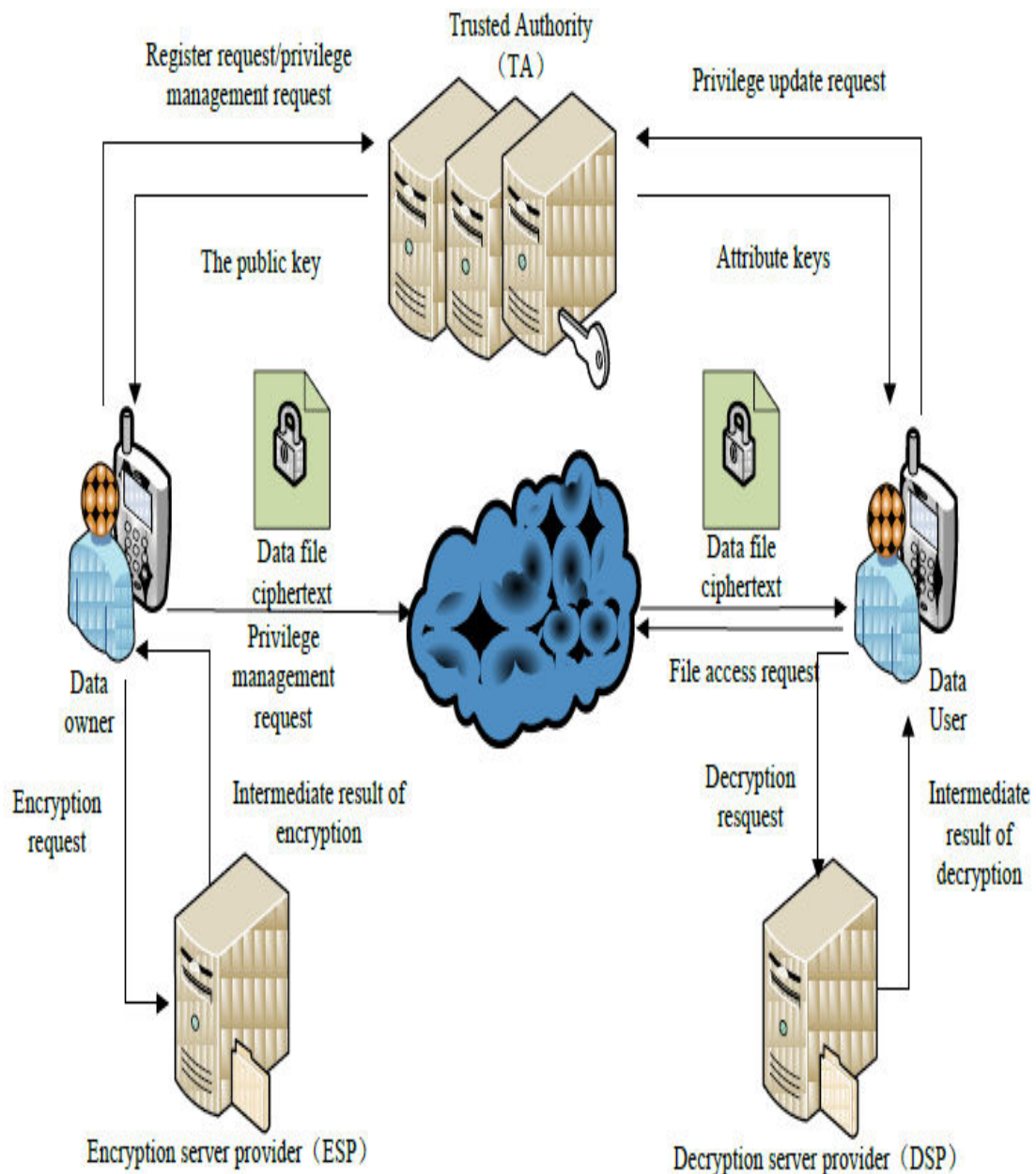


Fig:3.1 System Architecture

IMPLEMENTATION

MODULES:

Data User (DU):

Once the User enters into the application, he/she has to register. If the user is already registered then he/she can login using their login credentials. Before login the user as to be verified by the admin. DU logs onto the system and sends,an access request to Admin. Admin activates the request then user can view the encrypted file uploaded by the owner. Now user request for decryption key to download the files. When the key is sent then, DU decrypt the ciphertext of the symmetric key with the assistance of DSP. DU uses the symmetric key to decrypt the ciphertext of data files.

5 RESULTS AND DISCUSSION

SCREENSHOTS:

FIG:5.3.1 HOME PAGE

The screenshot shows the home page of a web application titled "A Lightweight Secure Data Sharing Scheme for Mobile Cloud Computing". The navigation bar includes links for Home, DATA OWNER, DATA USER, TRUSTED AUTHORITY, and CLOUD. The main content area features a collage of images related to mobile devices and cloud computing. Below the collage is a diagram illustrating the system architecture, showing a "Trusted Authority (TA)" receiving "Register request/privilege management request" and sending "Privilege update request" to "Attribute keys". The diagram also shows "The public key" and "Attribute keys" components. An "Abstract" section is visible on the right side of the diagram.

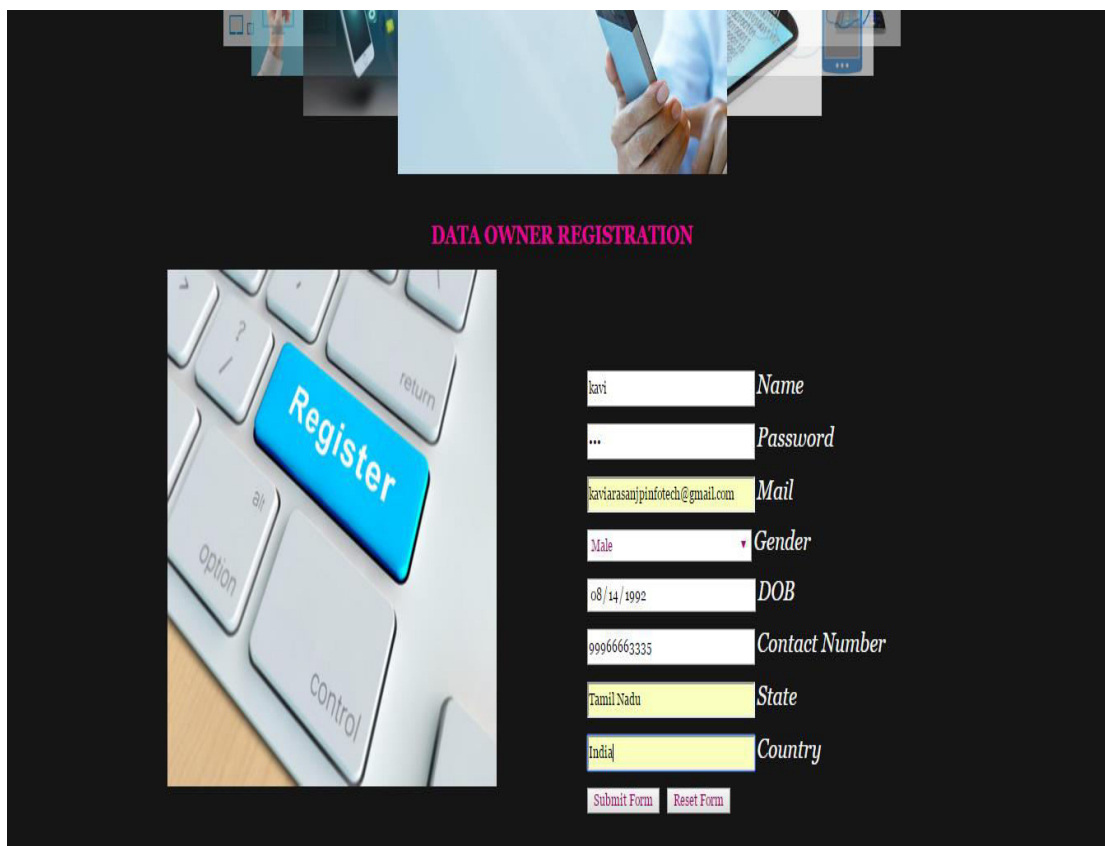
Abstract

With the popularity of cloud computing, mobile devices can store/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

localhost:8080/Lightweight_Secure_Data_Sharing_Scheme/ureg.jsp

FIG:5.1 HOME PAGE

FIG:5.3.2DATA OWNER REGISTRARTION:



DATA OWNER REGISTRATION

| | |
|-------------------------------|----------------|
| kavi | Name |
| ... | Password |
| kavirasanjpinfotech@gmail.com | Mail |
| Male | Gender |
| 08/14/1992 | DOB |
| 99966663335 | Contact Number |
| Tamil Nadu | State |
| India | Country |

**FIG:5.2
DATA**

OWNER REGISTRARTION

FIG:5.3.3 DATA OWNER LOGIN

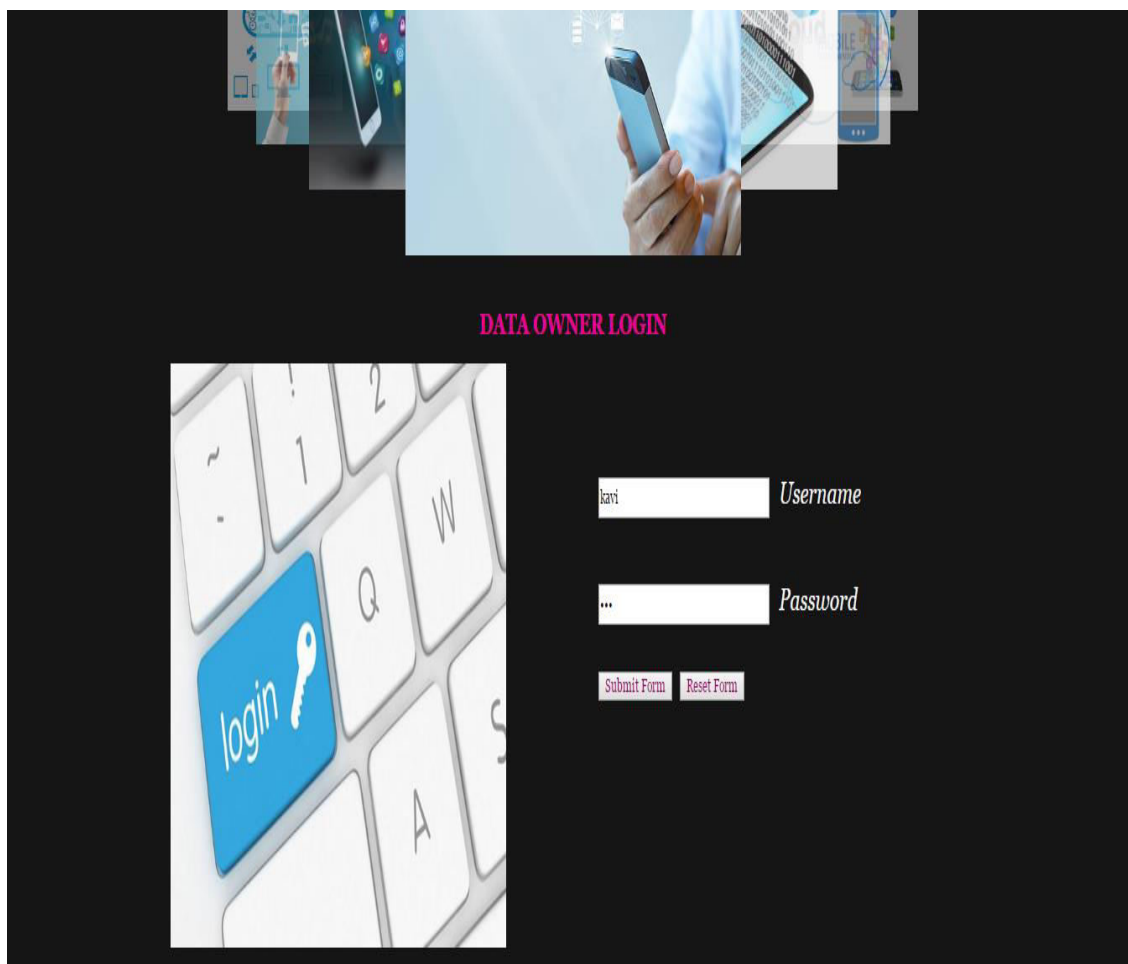


FIG:5.3 DATA OWNER LOGIN

FIG:5.3.4 PUBLIC KEY REQUEST

Public Key Request

| Id | Name | Mail | Status | Give Request |
|-----------|-------------|--------------------------------|---------------|---------------------|
| 1 | kavi | kaviarasanjpinfotech@gmail.com | Give Request | Request |

Note: If Status is Waiting means your request sent to TA but TA not yet Generate a Public key

Note: If Status is Update means you can Update your Public key

Menu Bar

- ▶ Home
- ▶ Public Key Request
- ▶ Upload File
- ▶ View Data User File Access Request
- ▶ View Uploaded Files
- ▶ Logout

**FIG:5.4
PUBLIC
KEY**

REQUEST

FIG:5.3.5 TRUSTED AUTHORITY LOGIN

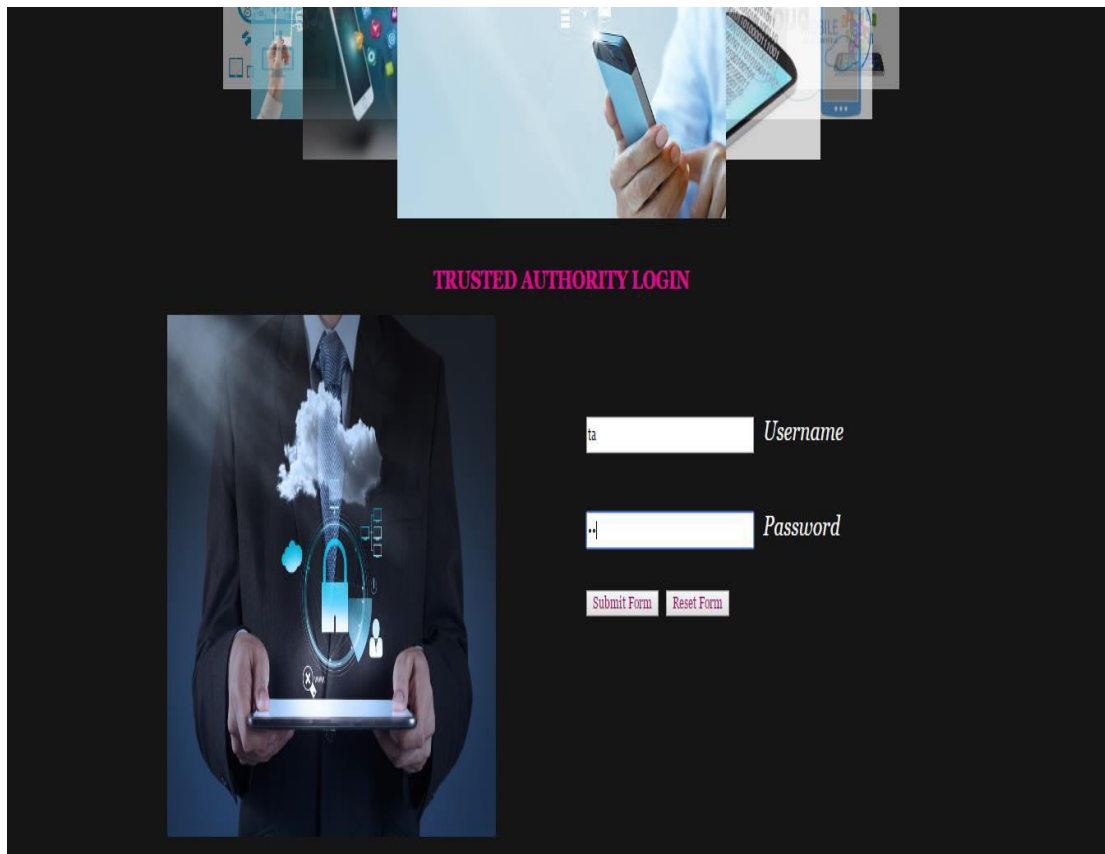


FIG:5.5

TRUSTED AUTHORITY LOGIN

FIG:5.3.6 TRUSTED AUTHORITY HOME

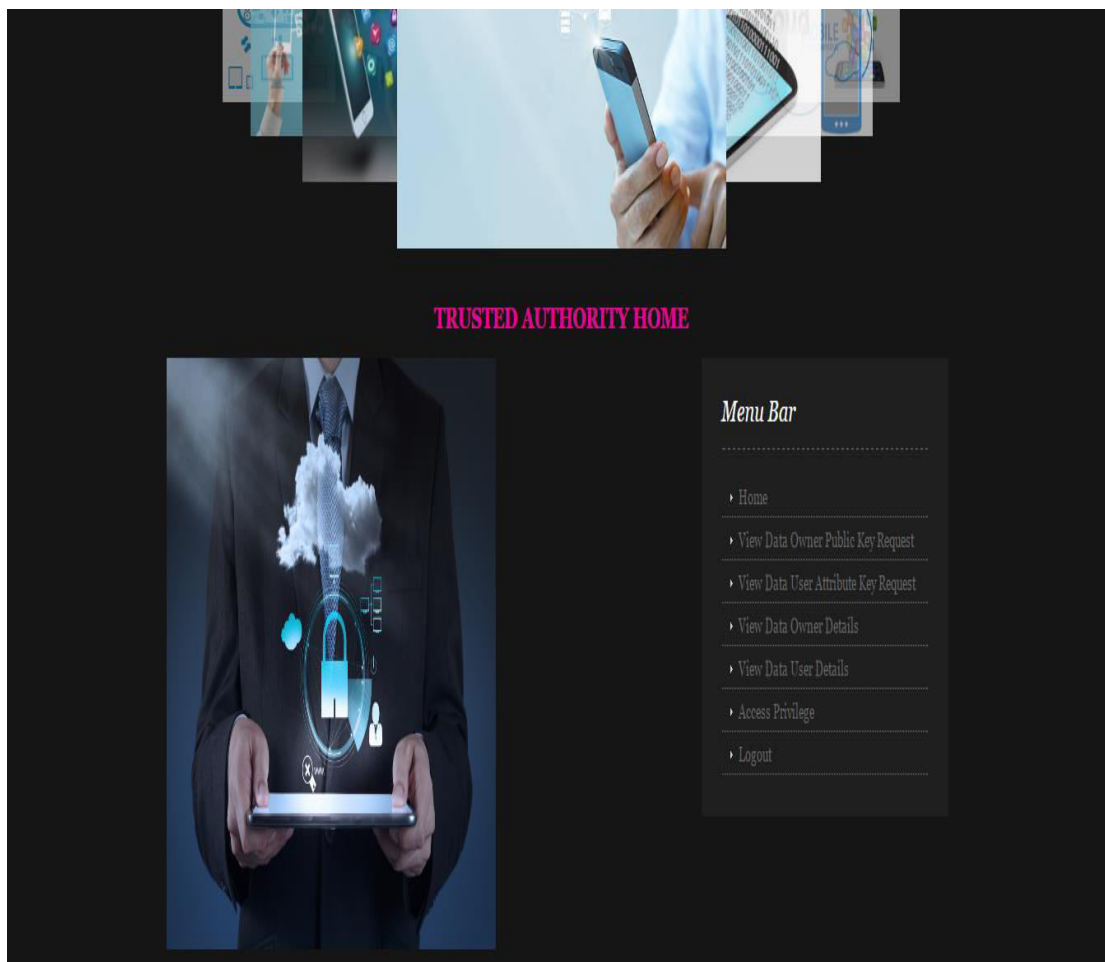


FIG:5.6

TRUSTED AUTHORITY HOME

FIG:5.3.7 DATA OWNER HOME:

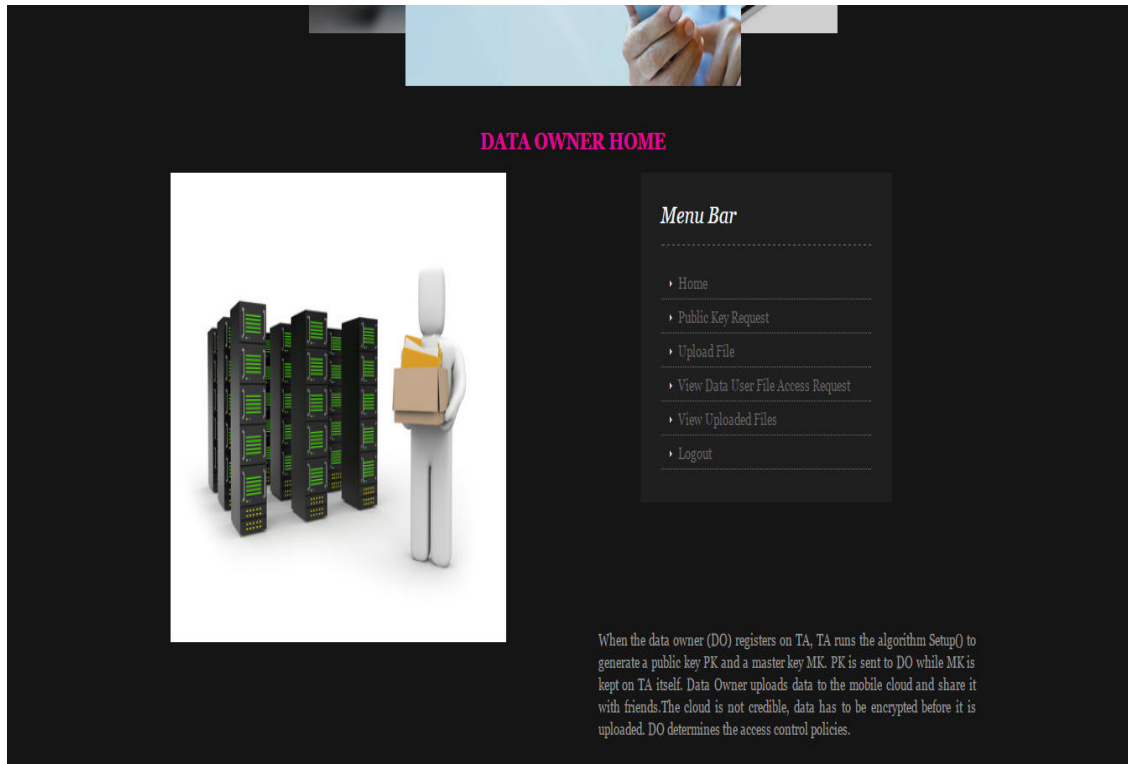


FIG:5.7 DATA OWNER HOME

FIG:5.3.8 CLOUD SERVER:



FIG:5.8 CLOUD SERVER

FIG:5.3.9 UPLOAD FILES:

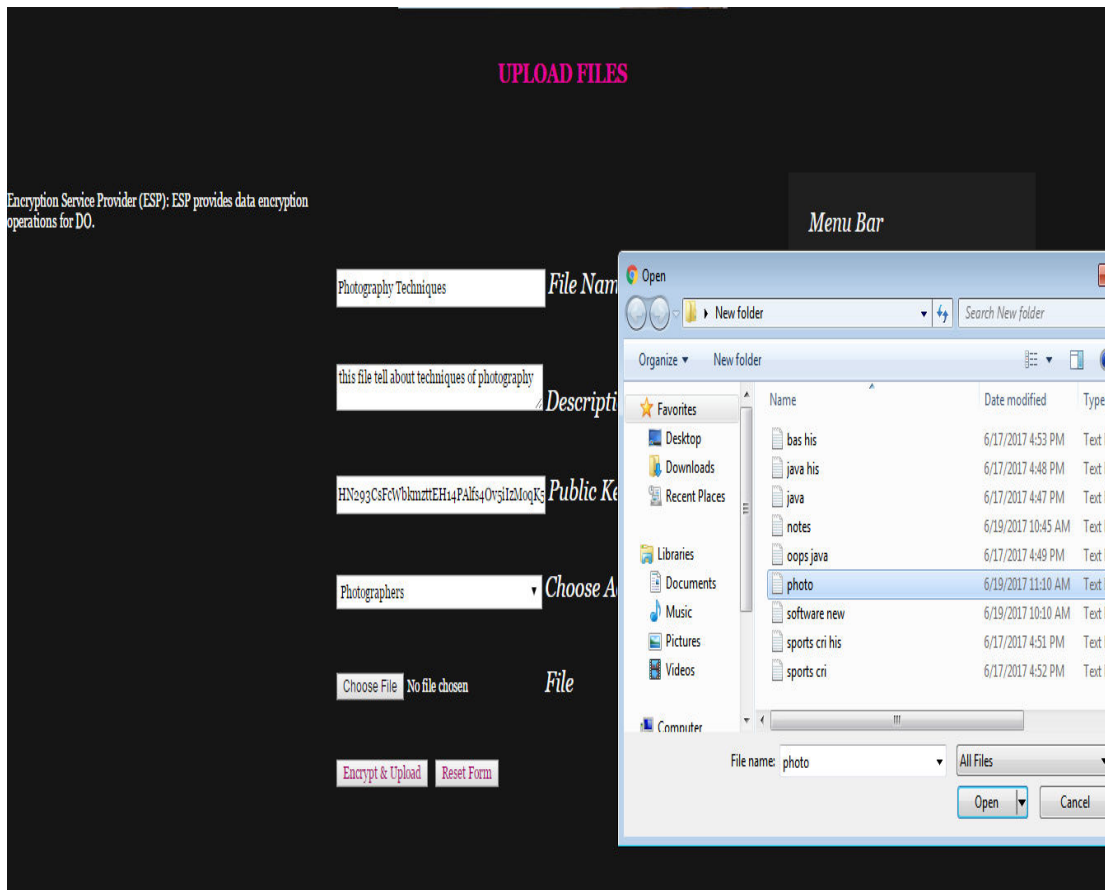


FIG:5.9

UPLOAD FILES:

FIG:5.3.10 DRIVE HQ:

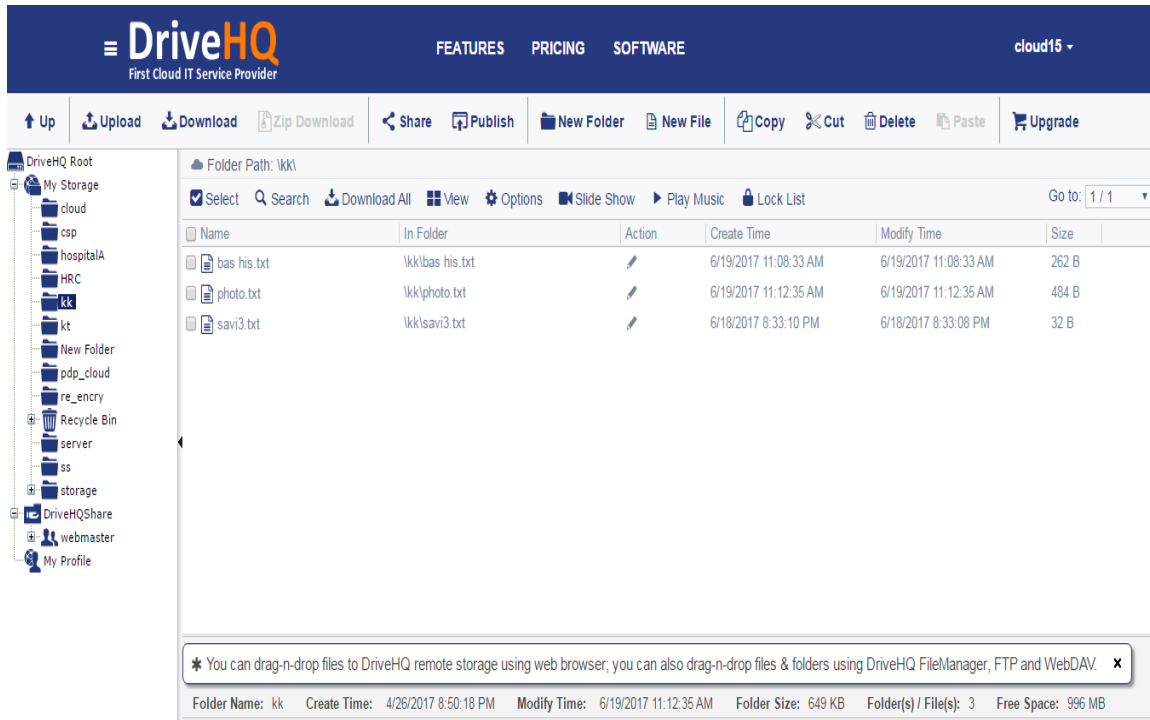


FIG:5.10 DRIVE HQ

FIG:5.3.11 VERIFICATION:

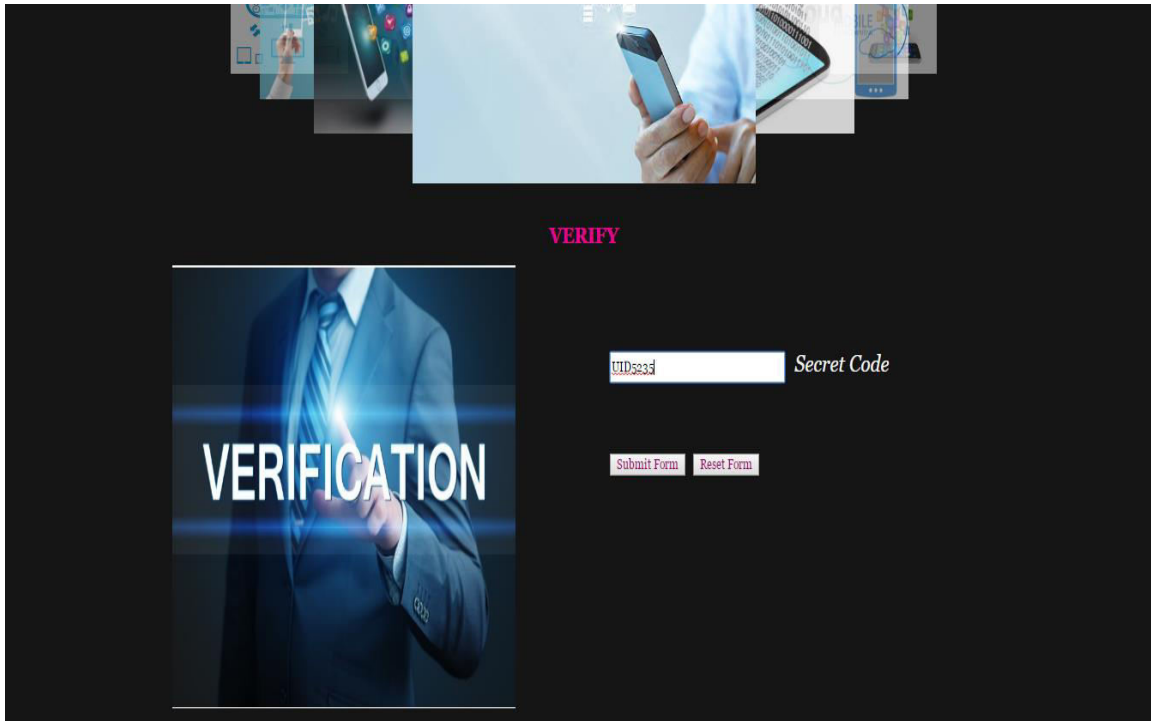


FIG:5.11 VERIFICATION

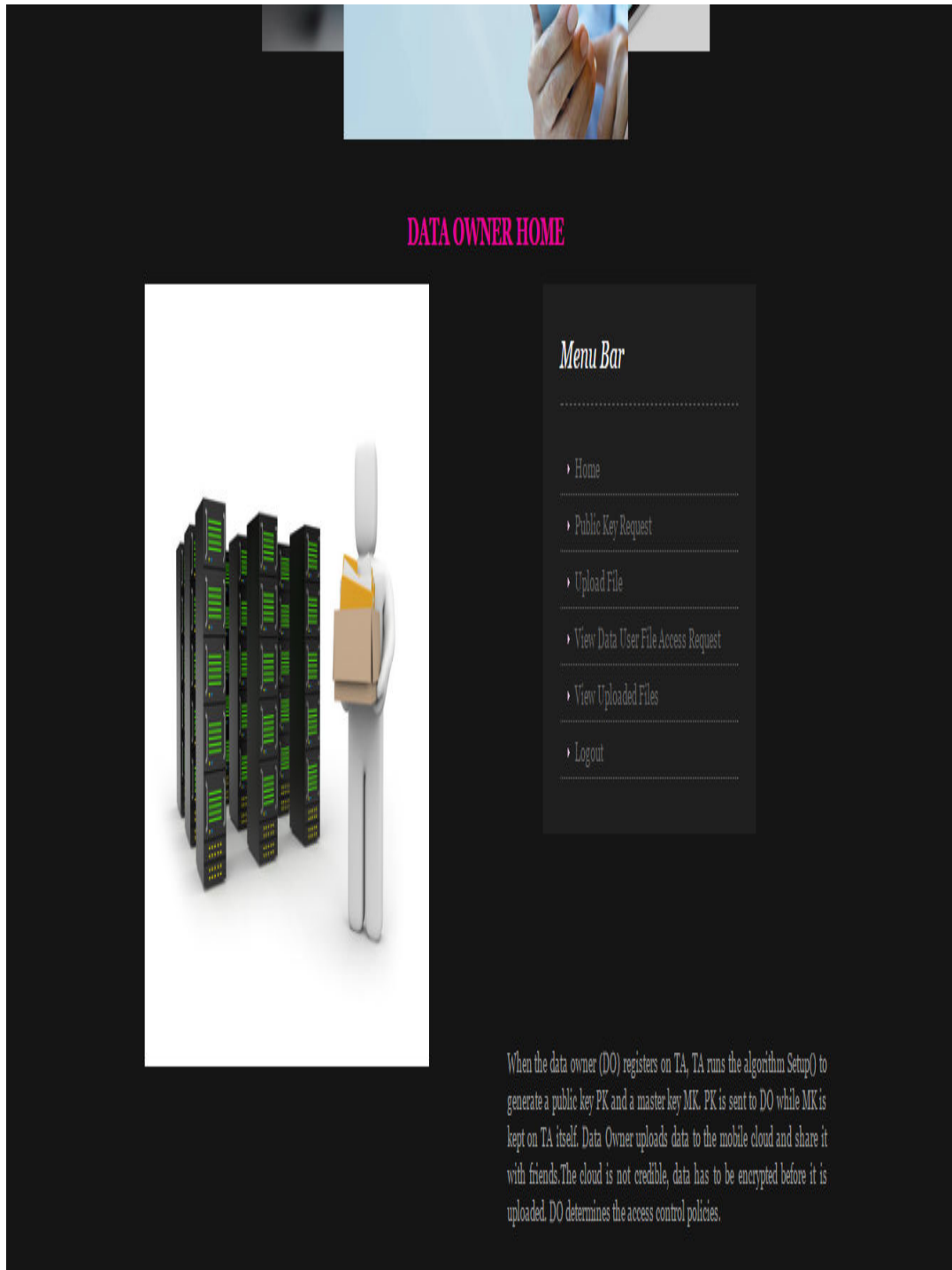
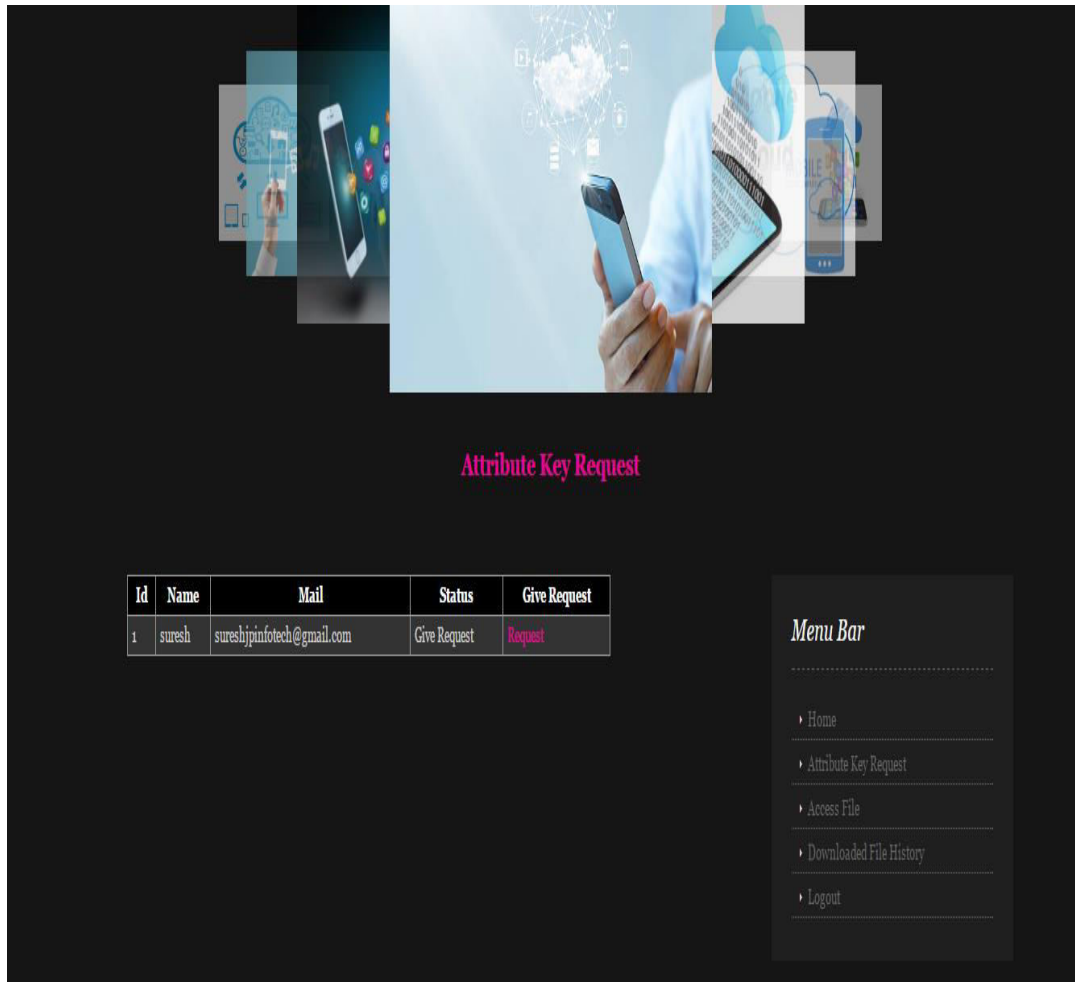
FIG:5.3.12 DATA OWNER MENU BAR**FIG:5.12 DATA OWNER MENU BAR**

FIG:5.3.13 ATTRIBUTE KEY REQUEST:**FIG:5.3.13 ATTRIBUTE KEY REQUEST****6. CONCLUSION AND FUTURE WORK****CONCLUSION**

In recent years, many studies on access control in cloud are based on attribute-based encryption algorithm (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 major computation overhead from mobile devices onto proxy servers, thus it can solve the secure data sharing problem in mobile cloud. The experimental results show that LDSS can ensure data privacy in mobile cloud and reduce the overhead on users' side in mobile cloud. In the future work, we

will design new approaches to ensure data integrity. To further tap the potential of mobile cloud, we will also study how to do ciphertext retrieval over existing data sharing schemes.

7. REFERENCES

- [1] 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.
- [2] 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.
- [3] Qihua Wang, Hongxia Jin. "Data leakage mitigation for discretionary access control in collaboration clouds". the 16th ACM Symposium on Access Control Models and Technologies (SACMAT), pp.103-122, Jun. 2011.
- [4] 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.
- [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: ACM pp. 55-66, 2009.
- [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-Volume 4*. USENIX Association, pp. 10-12, 2000.
- [7] Kan Yang, Xiaohua Jia, Kui Ren: Attribute-based fine-grained access control with efficient revocation in cloud storage systems. ASIACCS 2013, pp. 523-528, 2013.
- [8] Crampton J, Martin K, Wild P. On key assignment for hierarchical access control. in: *Computer Security Foundations Workshop*. IEEE press, pp. 14-111, 2006.
- [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)*, IEEE press, 2007. 350- 364
- [10] Cong Wang, Kui Ren, Shucheng Yu, and Karthik Mahendra Raje Urs. Achieving Usable and Privacy-assured Similarity Search over Outsourced Cloud Data. IEEE INFOCOM 2012, Orlando, Florida, March 25-30, 2012