International Journal of Combined Research & Development (IJCRD)
eISSN:2321-225X; pISSN:2321-2241 Volume: 14; Issue: 8; August- 2025

A LIGHT WEIGHT SECURE DATA SHARING SCHEME FOR MOBILE CLOUD COMPUTING

Shaik Mushrath Sulthana
PG, Student
Dept. of MCA
The Oxford College of Engineering,
Bommanahalli, Bengaluru- 560068
mushrathmca2025@gmail.com

Dharamvir
Assistant Professor
Dept. of MCA
The Oxford College of Engineering,
Bommanahalli, Bengaluru- 560068
hodmactoce@theoxford.edu

ABSTRACT

As mobile computing gains popularity, different companies have been considering establishing and operating cloud computing. remote storage of personal data can be accessed/retrieved anywhere by the user any time. It stops the additional as it becomes more intense. mobile cloud development. because mobile devices only have a limited amount of computing power and resources, the majority of the research will not apply to mobile cloud. Mobile cloud apps are highly sought after as solutions with low computational overhead. we present a (Lightweight data sharing scheme - LDSS). cloud computing on mobile It utilizes the CP-ABE which is an access . The design of such a environment for cloud of mobile should be DSS relocates A significant part of the regulation of access is computational. The design of such a mobile cloud environment should be DSS relocates A significant part of the access control is computational intensive of transformation in CP-ABE to mobile devices In addition to the processes involved in order to minimize the user. lazy-revocation, which is an unsavory problem in Besides that, optimistic biased questions regarding CP-ABE systems have been presented in a CP-ABE based signature scheme that, however, implements efficient CP-ABE systems.

Keywords: MCC, data encryption Access Select, User Revoke.

INTRODUCTION

Due to innovation around cloud computing and due to the widespread use of smart mobile devices. gradually adapting to the new paradigm for data sharing where data warehousing and storage is in cloud and the Data is stored and retrieved from the cloud using mobile devices. The computing power and available storage space of these devices is limited. Quite on the contrary, the cloud boasts

of tremendous resources. In a scenario like this, to meet the satisfactory performance levels, It is necessary for the product design must be made according to practical and effective application. It is critical to store the data, and distribute it to the use of the resources offered along cloud service provider(CSP). Mobile cloud applications have been in use. In such applications people.The data owners can post photos, videos, files, including documents, to the cloud and distribute them. This is done on the hope of sharing with other individuals (data-users) that like to share

The CSPs also offer data management Increased functionality to data owners. As the personal data files are sensitive, data owners have the option of selecting them.Whether locking their information files can be made open or restricted to only certain users of data. Of course, Many data owners are concerned with the privacy of the sensitive personal information data.The data owner can easily simplify the managing of the privilege by categorizing data users into different groups and deliver the password to groups they desire to share the data with. This method however necessitates fine-grained access control.

LITERATURE SURVEY

Controlling Acess is a binding aspect insurance for information security, to ensure that information can be accessed by legitimate users. There is abundant research for problem of information is taken over for primary focus of the most part has been on access authority over ciphertext, and the importance of access control .

Client approval effectively achieved through key dispersion The analysis can be generally divided into four areas: basic ciphertext access control, multiple leveled access control, access control though entirely homomorphic-encryption also property-based encryption-based access control (ABE).

Basic ciphertext get control refers to the the reality that following the encryption of information documents, the key to decryption is scattered safely in order to achieve approval to trusted clients. To reduce above large distribution of client keys; A technique known as Mobiflage was created by Skillen along with Mannan. which enables PDE (Hypothetically deniable encryption) in cellphones by storing coded volumes by using non-deterministic data on external storage of the gadget obtains the entry confinement course of action applied to

petite used appropriated storing, distinguishing the clients into different groups based on access rights and assigning different keys to groups. This reduces the overheads of major administration, but it cannot serve the need of fine-grained access control. An encryption can work so easily with the ciphertext. Its working results are the Leverages Entirely homomorphic - encryption as a form of calculation, thus being able to perform tasks such as recovery and calculation directly on ciphertext, all the information update is deceived by the clients.Activities related to change in benefits should be legal to do it on ciphertext.

EXISTING WORK

There four main classes of approaches that should be taken; important chip text regulation, sophisticated text regulation, advanced regulation of text, and critical regulation of text. And improved control management, and light of completely homomorphic encryption management. All these The poesie also is supposed to break out as unchanging state of the cloud. It was also proposed that its own new improvements should be introduced by ABE, where the latter assigned such increased control overheads against cryptography exercise, cloud supplier reduces aggravator communication expenses to that other end client. There is a need that the support data be obtained through required mobile phones. The confidentiality of an individual information is a real burden on the section data owners.

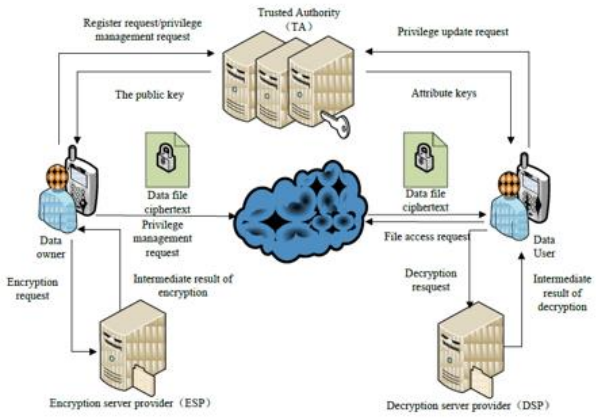
The mechanisms of the control reviewed by Toms CSP might not be adequate in the administration process. communal income. Each of them requires evidence of the claims of the data owners that they cannot do it. One of the things that stand out are true. The highly critical topic of consumer benefit transfer is one to which existing game strategies is applicable. or address .Any major rejection costs may fall on the shoulders of such a firm. The same is not the case with mobile phones. There is no possible strategy that can help to resolve the issue of sensitive information rapidly in the complex cloud.

PROPOSED SYSTEM

The proposed system recommend that you adoa Lightweight Information System (LDSS) keeping in view the common scattered nature. registration condition. Individual commitments of LDSS claims will be equivalent to all of the following: we will controlling as a ciphertext entity to be referred to in terms of a ciphertext

name, LDSS-CP-ABE in relation to assertions.

Methodology The research project is on the basis of attribute-based-encryption (ABE).We are, admittedly, performing encryption on normal servers. Certainly result of the door architecture, the data protection will remain, and hence the mentioned credit of LDSS-CPABE should be incorporated in the end result. We can apply this area of lethality re-encryption and representation in the denial of credits to this customer. Ultimately, we implement a multiple to depict the concept design with regards to the LDSS.

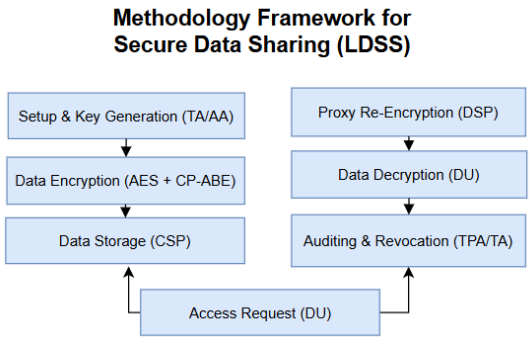


Fig(1):- Proposed System Workflow

METHODOLOGY

Our system will combine five modules that will make sharing data in the cloud to be secure and practical to the mobile users. The Lightweight CP-ABE Encryption Module enables data-owners to specify explicitly what person might access their data; this is then optimized, via the encryption service, in a manner that will minimize the load on the mobile devices. The same arrangement uses lazy revocation, in that when a user is removed they automatically have all access to newly encrypted files removed without the need to re-encrypt all files. The Attribute-Based Access Control Module also guarantees that the right users of the data have access through their attributes using a trusted authority prior to securely giving them decryption keys.

To ease access, the Proxy-Assisted Decryption Module does most of the burdensome decryption work on behalf of the mobile devices without making the access slow, and allows key protection via secure channels. The Lazy Revocation and Re-encryption Module maintains a high level of efficiency by only re-encryption files when files are modified, and version control prevents access by revoked users to updated data. Last, the Performance Optimization and Testing Module tests the system performance, the use of resources, and the capacity (i.e., scalability) of the systems under various circumstances, which proves that the lean system architecture using CP-ABE is the most effective system.



Fig(2):-

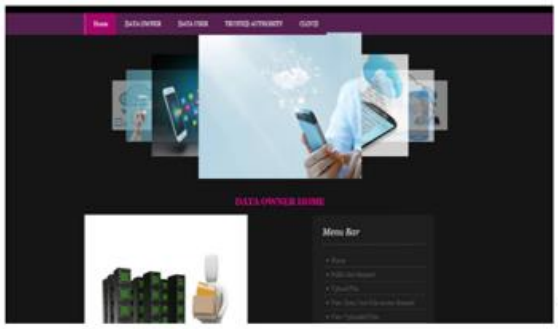
EXPERIMENTAL RESULTS

Present System includes An LDSS (lightweight data-sharing scheme) for mobile cloud's computing model where we employ proxy servers to carry out the encryption/decryption task. In our method, computationally expensive ABE tasks are executed by proxy servers, significantly reducing the computational load on mobile client side.

Fig (3) :- Home Page

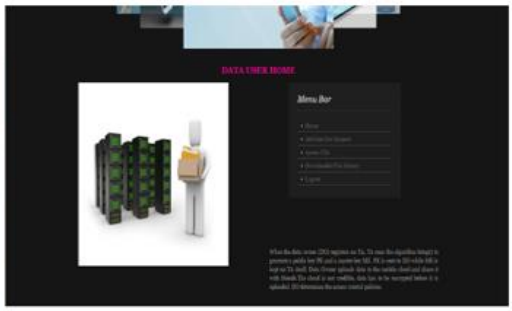
There are four modules such as data owner, data user, trusted authority, cloud.

Fig (4) :- Data Owner Page



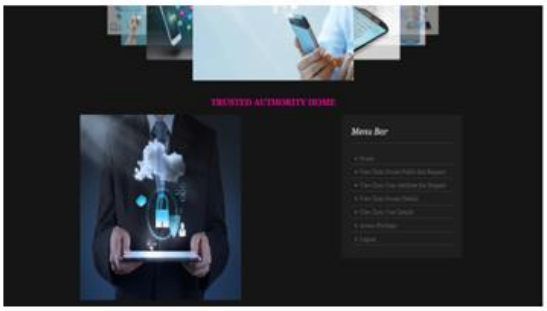
There are four fields public key request, upload file, view data user file access request, view uploaded files.

Fig (5) :- Data User Page



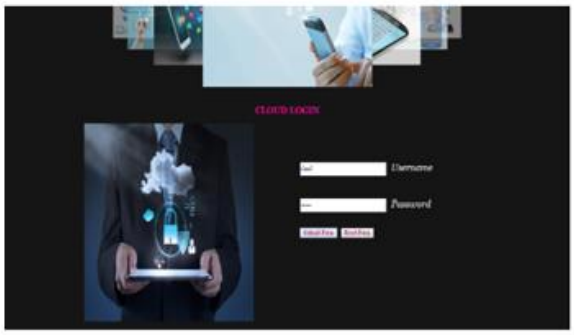
There are three fields attribute key request ,access files, downloaded file history.

Fig (6): - Trusted Authority page



There are five fields view data owner Pk request view data user attribute key request, view data owner details, view data user details, access privilege.

Fig (6): - Cloud page



There are three field s files and it' s access privilege , view files access request, files downloaded history.

CONCLUSION

In the recent years, several studies have been carried out in terms of access control. They are based on the attribute-based encryption, the innovation of which dates back to the works of Shmatikov and Tsudik in 2009 and Peikert and Waters algorithm (ABE). The conventional ABE is nevertheless It is not suited to mobile cloud.The extremely computationally intensive and mobile devices we cannot possibly possess but a certain number of resources..To deal with that issue, provided LDSS. It A novel scheme LDSS-CP-ABE on the basis of Lu-Du has been proposed in this paper.The major burden on mobile can be evaded by transferring a large burden of computation to mobile. It is capable of addressing these devices on servers that act as proxies, thus.

The problem of data sharing of mobile-cloud. Our results as indicated in our experiment show that (LDSS -proposed) can be used to ensure that. Enhance the privacy of the mobile-cloud and decrease the losses. There are some other costs incurred on the users who have to use mobile cloud.

REFERENCES

[1] Gentry C, Halevi S. Realizing the fully homomorphic encryption scheme of Gentry

[2] Adam Skillen and Mohammad Mannan. The use of mobile devices offers advantage provide Deniable storage Encryption.

[3] W, Li Z, Owens R, et al.Access to outsourced data in: Proceedings of the 2009A workshop on Cloud computing security

[10] Cong Wang, Kui Ren, Shucheng Yu, and Karthik Mahendra Raje Realizing Privacy and Usable Conditions in Similarity Search over Outsourced Cloud Data.

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

[9] De Shi E, Bethencourt J, Chan T H H, et al. Multidimensional range query over encrypted data. Proceeding of Symposium on Security and Privacy