A LIGHT WEIGHT SECURE DATA SHARING SCHEME FOR MOBILE CLOUD COMPUTING

G SURESH
Department Of Computer Science And Engineering, Visakha Institute Of Engineering And Technology,Visakhapatnam
g.suresh053@gmail.com

Y JAYALAKSHMI
Department Of Computer Science And Engineering, Visakha Institute Of Engineering And Technology,Visakhapatnam
yarangutla.jl@gmail.com

ABSTRACT

With the fame of distributed computing, mobile devices can store/recover individual information from anyplace whenever. Thusly, the information security issue in portable cloud turns out to be increasingly extreme and averts promote improvement of versatile cloud. There are generous examinations that have been directed to enhance the cloud security. In any case, the majority of them are not pertinent for portable cloud since mobile devices just have constrained registering assets and power. Arrangements with low computational overhead are in awesome requirement for versatile cloud applications. LDSS moves a substantial bit of the computational escalated calculation from mobile devices to servers. Once the information is transferred to the server it is then put away in scrambled configuration and can be decoded just with the authorization allowed by the trusted expert to the client who demand's the entrance. The test comes about demonstrate that LDSS can successfully decrease the overhead on the cell phone side when clients are sharing information in portable cloud situations.

INTRODUCTION

It is very important requirement that the documents of various formats sometimes need to be shared across group of people for the purpose of knowledge transfer, generation or a part of execution of a task. As the organization from educational to professional have been operating across the globe and are connected via internet and as the access of cloud infrastructure services has increased, it became a primary need. Now, sharing is not a major issue with the existing cloud infrastructures, but the concern is, its security and administrating its right to access. As a part of which it is also important to protect the content of those documents for unauthorized access which prevails to the preservation of the document owners economic or it interests.

This project is demonstration of the above explained, exhibits how protective administration of file access shared on public or private clouds can be achieved, by incorporating encryption algorithms and indecently generates keys where the execution time optimization and the hardness of key predicting are primary interests. Execution time optimization is a concern as the files must be accessible via a cloud that can be pinged from even devices that are not computationally heavy like Mobiles.

This project is a cloud environment where students of specific educational organization can share their documents and that list of documents are visible to rest of all the members of that

organization. These documents are encrypted through Ecliptic Curve Cryptography and if anyone tries to download these documents, it will be delivered only in encrypted format.

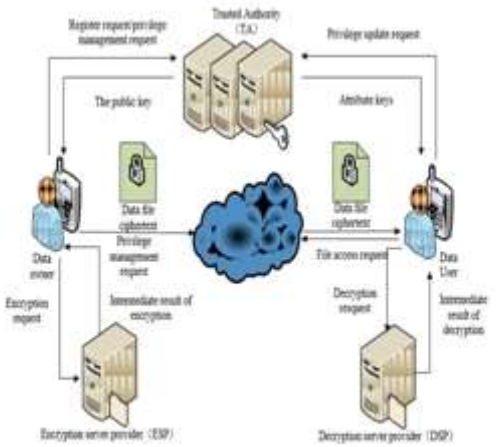

Fig 1.1: A lightweight data-sharing scheme (LDSS) framework.

To decrypt these documents the interested member has to raise a access request to the admin of the site, and the admin will have to grant the request, and only those members who got the access granted can download the decrypted form of the documents. The figure above depicts the framework for the proposed lightweight data sharing scheme, where a the data owner uploads the data which gets encrypted and then the data user request the access to the data which is done by a trusted authority who provides the keys for encryption and decryption

LITERATURE SURVEY

A literature review is a description of the literature relevant to a particular field or topic. It gives an overview of what methods and methodologies are appropriate and useful. As such, it is not in itself primary research, but rather it reports on other findings. A literature review may be purely descriptive, as in an annotated bibliography, or it may provide a critical assessment of the literature in a particular field.

Mobile device has limited storage and limited computing resources so mobile cloud can be utilized to store data which allows user to access the data from anywhere and from anytime. Since cloud storage are publicly available and accessed by many, there lies a security issue related to data hence it becomes a serious need to provide security to the data to prevent being accessed or misused from unauthorized user.

FUNCTIONALITIES:

It uses **Elliptic Curve Cryptography** algorithm for encryption and decryption of the data.

The User uploads data to the mobile cloud and shares it with everyone over the application. In order to access these files other users have to create a new request to the admin of the site and once permission is granted they'll be able to access those files.

Trust Authority (TA): TA grants access permission to the user who requested for accessing the file. The TA is responsible for granting and denying the services to the users who created the request also he manages the accounts of the users in the enrolled to the application.

Encryption Service Provider provides data encryption operations for uploaded data by the user whereas Decryption Service Provider provides data decryption operations for the data which is to be

downloaded by users. These services are provided by the cloud server deployed.

FEATURES:

Lightweight data sharing scheme technique enables mobile device to share data easily over the cloud. The data shared over the cloud can be access from anywhere with help of internet.

The security of user's privacy is maintained by administrator as the password of the users account stored in database is hashed. The access control system enables only the authorized user to access to the data. The files uploaded are encrypted using elliptic curve cryptographic algorithms. Unauthorized download of a file i.e., downloading a file without the access of the administrator will download the file in encrypted format and hence the user won't be able to use the file.

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.

EXISTING SYSTEM:

With 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.

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.

PROPOSED SYSTEM:

Apparently, to solve the above problems, personal sensitive data should be encrypted before uploaded onto the cloud so that the data is secure against the CSP. However, the data encryption brings new problems. How to provide efficient access control mechanism on cipher text decryption so that only the authorized users can access the plaintext data is challenging. In addition, system must offer data owners effective user privilege management capability, so they can grant/revoke data access privileges easily on the data users. There have been substantial researches on the issue of data access control over cipher text. In these researches, they have the following common assumptions. First, the CSP is considered honest and curious. Second, all the sensitive data are encrypted before uploaded to the Cloud. Third, user authorization on certain data is achieved through encryption/decryption key distribution. In general, we can divide these approaches into four categories: simple cipher text 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.

CONCLUSION

In recent years, many studies have been carried out to provide a cloud which is secure and is also easily available to all, also many studies on access control in cloud are based on attribute-based encryption algorithm however, not all the specified algorithms are suitable for the mobile cloud because it is computationally intensive and mobile devices only have limited resources.

In this project, we propose LDSS to address this issue. It introduces a novel LDSS with ECC algorithm to migrate major computation overhead from mobile devices onto the cloud 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.

REFERENCES

1. N. Khan, M. L. M. Kiah, S. U. Khan, and S. A. Madani, "Towards secure mobile cloud computing: A survey," Future Gen. Comput. Syst., vol. 29, no. 5, pp. 1278– 1299, Jul. 2013

2. C Shravanthi, H S Guruprasad,"Mobile cloud computing as future for mobile applications",ijret: international journal of research in engineering and technology eissn: 23191163 | pissn: 2321-7308

3. A. Cecil Donald, S. Arul Oli, L. Arockiam ,"Mobile Cloud Security Issues and Challenges: A Perspective", International Journal of Engineering and Innovative Technology (IJEIT) Volume 3, Issue 1, July 2013

4. L. Wei, H. Zhu, Z. Cao, Y. Chen, and A. V. Vasilakos, "Security and privacy for storage and computation in cloud computing," Inf. Sci., vol. 258,371–386, Feb. 2014.

5. Wei Ren et al, "Lightweight and Compromise Resilient Storage Outsourcing with Distributed Secure Accessibility in Mobile Cloud Computing", ISSNll1007-0214ll06/09llpp520-528 Volume 16, Number 5, October 2011.