A LIGHTWEIGHT SECURE DATA SHARING SCHEME FOR MOBILE CLOUD COMPUTING

Keerthi G [1], Dr K N Shreenath[2]

P.G Student, MTech, Computer Networks Engineering, Department of CSE, Siddaganga Institute of Technology, Tumkur, India[1],

Associate professor, Department of CSE, Siddaganga Institute of Technology, Tumkur, India [2]

Abstract: Cloud storage is simple and scalable way to store, access and share data over the Internet. Consequently, data security problems are becoming more and more severe and prevent further development of mobile cloud. There are several studies that have been done to improve the cloud security. However, most of them are not applicable for mobile cloud since mobile devices have less computing resource and power. Solution with low computational overhead is in great need for mobile cloud applications. In this paper, we propose a Lightweight data sharing scheme (LDSS) for mobile cloud computing. It adopts Cipher Policy- Attribute Based Encryption (CP-ABE), an access control technology used in normal environments, but it changes the structure of access control tree to make it suitable for mobile cloud computing. LDSS moves large portion of the computational intensive access control tree transformation in CP-ABE from mobile devices to external proxy servers. Attribute based encryption (ABE) is used to for cloud storage security.

Index Terms: **ABE, Mobile cloud computing, data encryption and decryption, access control.**

I. Introduction

Cloud computing provides us a means by which we can access the applications as utilizes, over the Internet. It allows us to create, configure, and customize applications online. With the cloud computing users can access the database resources via the internet from anywhere as long as they need without worrying about the maintenance or management of actual resources. Cloud refers to network or internet. We can say the cloud is something, which is present at remote location. Cloud can provide services over network i.e., on private and public cloud networks i.e. WAN, LAN or VAN. Applications such as E-mail, web conferencing, customer relationship management all run in cloud. Cloud computing is both software and hardware based computing resources delivered on a network services.

With the development of the cloud computing and the popularity of smart mobile devices, people are getting familiar to the new era of data sharing in this we store, retrieve the data from the cloud. As we know that mobile devices have very less storage capacity and computing power, but cloud has large amount of resource. In the scenario, to achieve satisfactory performance it is essential to use the resource provided by the cloud service provider (CSP) to store and share the data. In recent days cloud mobile applications are most widely used. In these applications data owner can upload their documents, photos, videos and other files to the cloud and share the data with data users. CSPs also provide data management functionality for data owners. Since the personal data files are sensitive DO has to make sure that whether to make the data public or to share only with specific data users. It very important to provide data privacy and the data security which is major concern.

The control mechanism provided by the CSP is not sufficient as it doesn't meet all the requirements of the data owner. Firstly whenever the user upload the files to the cloud they are leaving their files where there is no control over it there may be chances of spying on the files that causes the privacy problems. Later the user can send the passwords for the encrypted files to unlock it. To overcome from all these problems the data owner can divide the data users into group and he can share the password with particular group. Password management is great issue for the security.

Many studies have been done on the issue of data access control over cipher text. In these studies they have the following assumptions. Firstly the CSP is considered as honest and curious. Second, all the sensitive data should be encrypted before sending it to the cloud. Third, user authorization on certain data is achieved through encryption/ decryption key distribution.

In general, we can divide these applications into four categories: simple cipher text access control, hierarchical access control, access control based on fully homomorphic encryption access control and access control based on attribute-based-encryption (ABE). All these approaches are designed for non-mobile cloud environment. They consume large amount of storage and computational resources, which are not available for mobile devices. Clearly, there is no solution which can effectively solve the secure data sharing problem in the mobile cloud. As the mobile cloud becomes more and more popular, providing an efficient secure data sharing mechanism in mobile cloud is in urgent need.

To address this issue, in this paper we proposed a lightweight data sharing scheme (LDSS) for mobile cloud computing environment.

Benefits of cloud computing:

The following are some of the possible benefits for those who offer cloud computing-based services and applications.

- **Cost Savings**: Companies can reduce their capital expenditures and use operational expenditures for increasing their computing capabilities. This is a lower barrier to entry and also requires fewer in-house IT resources to provide system support.
- **Flexibility**: The flexibility of cloud computing allows companies to use extra resources at peak times, enabling them to satisfy consumer demands.
- **Reliability**: Services using multiple redundant sites can support business continuity and disaster recovery.
- **Maintenance**: Cloud service providers do the system maintenance, and access is through APIs that do not require application installations onto PCs, thus further reducing maintenance requirements.
- **Mobile Accessible**: Mobile workers have increased productivity due to systems accessible in an infrastructure available from anywhere.

II. LITERATURE SURVEY

The author in [1], proposed Attribute Based Encryption (ABE).ABE is divided 2 categories: Control Policy-Attribute Based Encryption (CP-ABE), in which the access controls policy is embedded into cipher text. Key Policy-Attribute Based Encryption (KP-ABE), in which the access control policy is embedded into user's key attributes. In ABE cipher text is not encrypted to one particular user as in traditional public key cryptography. Instead both user's private key and cipher texts will be associated with a set of attributes or a policy over attributes. The user can decrypt the cipher text if there is a match between his private key and the cipher text.

The author in [2],"survey on lightweight secure data sharing scheme for cloud computing", the main problem faced by everyone is to share the data securely all over the world or at organization level. To overcome from this problem and to share the data securely they have used the combination of Attribute Based Encryption and Byte Rotation Encryption algorithm for encrypting the mobile data for sending on the cloud. It will help the user to securely store and share the data in encrypted form.

The author in [3], "A data security framework for mobile cloud computing ", In this Paper they have proposed security frameworks that will focus on reducing the complexity of cryptographic algorithms or different methods to offer confidentiality and security.

The author in [4],"Achieving usable and privacy assured similarity search over outsourced cloud data", In this paper authors have investigated on the problem of secure and efficient similarity search over outsourced cloud data. Similarity search is a fundamental and powerful tool widely used in plaintext information retrieval.

The author in [5], "Effective data access control for multi-authority cloud storage systems", In this paper authors have proposed DAC-MACS (Data access control for Multi-Authority Cloud Storage), this is an effective and secure data access control scheme with efficient decryption and revocation and multi-authority CP-ABE scheme was construed to achieve forward and backward security.

User authorization is achieved through key distribution. The research can be generally divided into four areas: simple cipher text access control, hierarchical access control, access control based on fully homomorphic encryption access control and access control based on attribute-based-encryption (ABE).

The author in [6], Simple cipher text access control refers to that after data file encryption, the encryption keys are distributed in a secure way to achieve authorization for trusted users.

Author in [7], to reduce the overhead of massive user key distribution, they designed a system called Mobiflage that enables PDE (plausibly deniable encryption) on mobile devices by hiding encrypted volumes via random data on devices external storage. However, the system needs to obtain large amount of keys.

Author in [8], borrows the access control method used in conventional distributed storage, separating users into different groups according to access rights and assign different keys to groups. This reduces the overhead of key management.

Author in [9], Hierarchical access control has god performance in reducing the overhead of key distribution in cipher text access control. As a result there have been done many researches on on cipher text access control based on hierarchical access control method. In this access control method, keys can be derived from private keys and public keys and a public token table.

Author in[10], full homomorphic encryption algorithm can operate directly on the cipher text. Its operation results are the same with operating on plaintext and then encrypting the data.

III. BACKGROUNG STUDY

Mobile cloud computing (MCC) fig 1 is the combination of two computing technologies: 1) Mobile cloud computing and 2) Cloud computing. MCC is defined as Cloud Computing Extended by mobility and a new Ad-Hoc Infrastructure based on mobile devices. Mobile cloud computing inherits the advantages and services of cloud computing

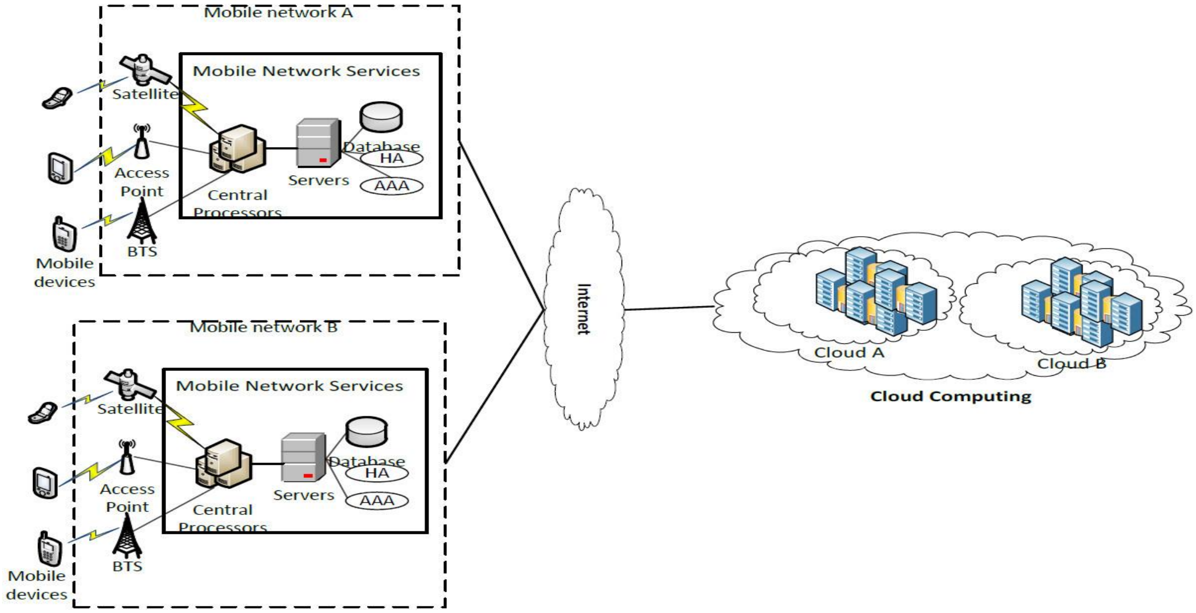

Figure 1 Mobile cloud computing

Cloud computing (figure 2) refers to both the applications delivered as services over the Internet. The software and hardware in the cloud computing architecture are largely kept on servers on the web or clouds and not in individual computers, through the internet. As essential aspect of the cloud is availability of the different types of data on the cloud platform. The main feature of cloud computing is to store lots of confidential data and personal information of users. Hence, the cloud service must provide automation and security to the users

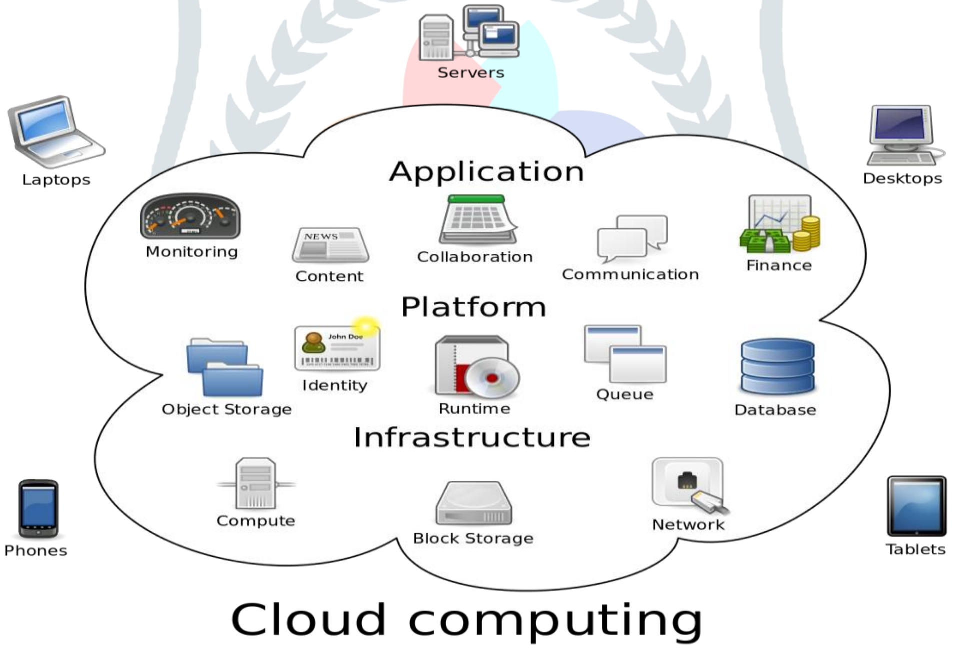

Figure 2 Overview of cloud computing

The goal of Cloud computing is to enhance the computational capacity of the cloud system to increase the access levels to the services and resources of the cloud at relatively low cost. The mobile users may utilize the computational power and storage capability of cloud for executing the computationally exhaustive and storage demanding processes of an application. The main objective of the mobile cloud computing is to reduce the energy consumption, when perform the computationally intensive tasks and to increase the mobile devices processing power and storage capabilities.

IV. Existing System

In current proposals on data access control in the cloud are mostly for non-mobile terminals, which is not suitable for mobile devices.

Existing studies on mobile cloud don't have a good solution to secure data sharing when servers are not credible. In a word, there is no proper solution that can solve the problem of secure data sharing in mobile cloud.

Because of these security issues there was a problem in the existing system to share the data securely, in this paper we propose a lightweight data sharing scheme (LDSS) for mobile cloud applications to share the data securely. It adopts CP-ABE, a technology used in access control in the normal cloud environment, but changes the structure of access control tree to make it suitable for mobile cloud. LDSS is provably secure, and is demonstrated to be more efficient and scalable.

V. METHODS AND TECHNIQUES USED

In Proposed System, we use LDSS-CP-ABE algorithm, this Algorithm designed using following methods.

i. Setup (A, V)-It generate the private master key and public key on set of attributes A of the data owner and version attribute V.
ii. KeyGen (Au, MK)-It is used to generate attribute keys SK for data user based on attribute set A and master key MK.
iii. Encryption (K, PK, T)-Based on symmetric key K, Public key PK and Access Control tree T generate cipher text CT.
iv. Decryption (CT, T, SK)- Attribute Key SK and Access control tree. It decrypt cipher text CT.

LDSS is nothing but the one type of technique which provides security to the lightweight data sharing scheme on mobile cloud. In LDSS it uses attribute based encryption which has another two subparts in it:

- CP-ABE:-Cipher text policy Attribute based Encryption.
- KP-ABE:-Key Policy Attribute based Encryption.

PROPOSED SYSTEM

In the proposed system, we develop the architecture of LDSS by using following six components.

1. **Data owner (DO):** The main responsibility of the data owner is to upload the file to the cloud. And he can able to see the uploads of different owner.
2. **Trusted authority (TA):** Trusted authority is responsible for generation keys and distributing he will having rights to add or delete a file.
3. **Data User (DU):** The user can able to view the list of files which are uploaded by the owner, and if he wants to download the files user has to send a key request to the authority, once the TA sends key to the data user he can download the file.
4. **Encryption server provider (ESP):** ESP provides data encryption operations for DO.
5. **Decryption server provider (DSP):** DSP provides data Decryption operations for DU.
6. **Cloud services provider (CSP**): CSP store the data for DO. It faithfully executes the operations requested by the DO, while it may peek over data that DO has stored in the cloud.

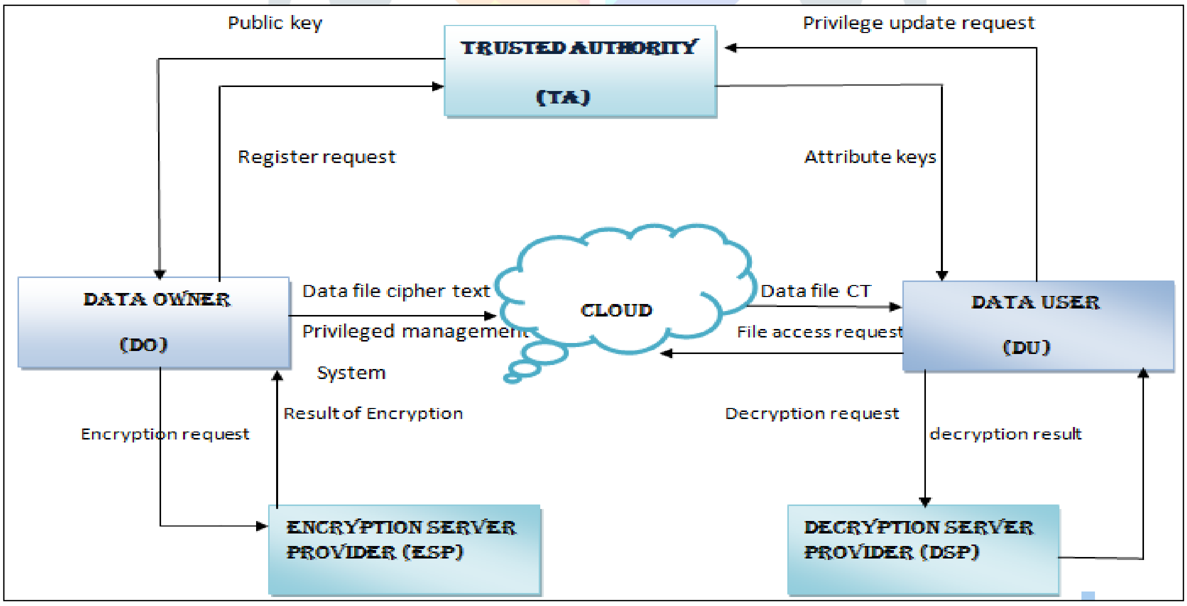

Figure 3: A Lightweight data-sharing scheme (LDSS) framework

As shown in the figure 3, a DO sends data to the cloud. Since the cloud is not credible, data has to be encrypted before it is uploaded to the cloud. The DO defines access control policy in the form of access control tree on data files to assign which attributes a DU should obtain if he wants to access a certain data file. In LDSS, all the files are encrypted with the symmetric encryption mechanism, and the symmetric key for data encryption is also encrypted using attribute based encryption (ABE).the access control policy is embedded in the cipher text of the symmetric key. Only a DU who obtains attribute keys that satisfy the access control policy can decrypted the cipher text and retrieve the symmetric key. As the encryption and decryption are both computationally intensive, they introduce heavy burden for mobile users. To relive the overhead on the client side mobile devices, encryption server provider (ESP) and Decryption server provider (DSP) are used. Both ESP and DSP are semi-trusted.

VI. Conclusion

In this paper we have presented a novel secure information management architecture and implementation and proposed a framework LDSS for secure sharing of data on mobile cloud, also we can use Advance Encryption Standard (AES) for perform encryption and decryption of data. The exploratory results show that LDSS can ensure data security in convenient cloud and lessening the overhead on customers' side in flexible cloud. Also we refer Third Party Authorization (TPA) for authentication purpose. By using TPA we can check integrity of related files which are uploaded by data owner.

References

1. Sahai, H. Seyalioglu, and B. Waters, “Dynamic credentials and ciphertext delegation for attribute-based encryption,” in Advances in Cryptology–CRYPTO 2012. Springer, 2012.
2. Shubham Chandugade ,”survey on lightweight secure data sharing scheme for cloud computing”, International Research Journal of Engineering and Technology (IRJET)-ISSN: 2395-0056 Volume: 04 Issue: 10 Oct 2017 .
3. Chandi patel,sameer singh, “A data security framework for mobile cloud computing “,International Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 2, February 2015.
4. Xinyu Wang,Kui Ren karthik Mahendra Raje Urs [4],”Achieving usable and privacy assured similarity search over outsourced cloud data”, published in proceeding IEEE INFOCOM 2012 DOI:10.1109 /INFCOM 2012.6195784.
5. Kan Yang, XiaohuaJia, Kui Ren ,”Attribute-based fine-grained access control with efficient revocation in cloud storage systems”, ASIACCS 2013, pp. 523-528, 2013.
6. 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.
7. 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.
8. 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.
9. D. Huang, X. Zhang, M. Kang, and J. Luo. Mobicloud: A secure mobile cloud framework for pervasive mobile computing and communication. in: Proceedings of 5th IEEE International Symposium on Service-Oriented System Engineering. Nanjing, China: IEEE, pp. 90-98, 2010.
10. Benjamin Livshits, Jaeyeon Jung. Automatic Mediation of Privacy-Sensitive Resource Access in Smartphone Applications. USENIX Security, pp.113-130, Aug. 2013.
11. Zhou Z, Huang D. Efficient and secure data storage operations for mobile cloud computing. in: Proceedings of 8th International Conference on Network and Service Management (CNSM 2012), Las Vegas, USA: IEEE, pp. 37-45, 2012.
12. P. K. Tysowski and M. A.Hasan. Hybrid attribute- and re-encryption-based key management for secure and scalable mobile applications in clouds. IEEE Transactions on Cloud Computing, vol. 1, no. 2, pp. 172-186, Nov. 2013.
13. .Ruixuan Li, Member, IEEE, Chenglin Shen, Heng He,Xiwu Gu Zhiyong Xu, and Cheng-Zhong Xu, Member, IEEE,” A lightweight secure data sharing scheme for mobile cloud computing”, IEEE TRANSACTION ON CLOUD COMPUTING, VOL 6, NO 2, APRIL-JUNE 2018 .
14. Princy P.James, Renuka Ajay Sonon, Naveen Ghorpad, Reddy kumar,”An efficient lightweight secure data sharing scheme for mobile cloud computing”, International Journal of Innovative Research in Science, Engineering and Technology An ISO 3297:2007 Certified Organization Volume 7, special Issue 6 ,May 2018.
15. 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: ACM press pp. 261-270, 2010.
16. 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.
17. 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.