INTERNATIONAL JOURNAL FOR INNOVATIVE RESEARCH IN MULTIDISCIPLINARY FIELD ISSN: 2455-0620 Volume - 6, Issue - 3, Mar – 2020
Monthly, Peer-Reviewed, Refereed, Indexed Journal with IC Value: 86.87 Impact Factor: 6.497
Received Date: 20/03/2020 Acceptance Date: 30/03/2020 Publication Date: 31/03/2020

An efficient Secure Lightweight Data Sharing Approach for Mobile Cloud

[1]Jebakumari M., [2]Ganesh S , [3]Kotamraju Uday Vamsi Krishna , [4]Prathap J.
[1] Associate Professor, [2, 3, 4] UG Scholars, Department of Computer Science and Engineering ,
Nehru Institute of Technology, Coimbatore, India
Email – [1]jebs1967@gmail.com, [2]ganeshreddy2611@gmail.com,[3] vamsikotamraju@gmail.com ,
[4]prathapj1998@gmail.com,

Abstract: *With the advancement in Cloud Computing, mobile devices can store and retrieve data from anywhere at any time. However, data security problem in mobile cloud turns out to be more severe and this prevents further growth of mobile cloud. Though a lot of studies have been conducted to improve the cloud security, most of them are not applicable for mobile cloud since mobile devices have only limited computing resources and power. Hence, solutions that involve low computational overhead are in immense want for mobile cloud applications. In this paper, a lightweight data sharing scheme (LDSS) for mobile cloud computing is proposed which adopts the access control technology, Ciphertext-Policy Attribute-Based Encryption (CP-ABE) used in cloud environment; but the structure of access control tree is altered to make it apt for mobile cloud environment. The experimental results show that the proposed approach effectively decreases the overhead on the side of mobile devices while users share data in mobile Cloud environment.*

Keywords : *Lightweight Data Sharing Scheme (LDSS),Mobile Cloud, Access control***.**

1. INTRODUCTION:

Smart mobile devices have become ubiquitous and the global community is steadily getting accustomed to doing everything with mobile devices. In this new era of smart living, novel data sharing models come up to assist us in several ways. One such data sharing model using smart devices aims at storing and retrieving data in the cloud. Typically, mobile devices have only limited storage space and computing power while the cloud has enormous amount of resources. In order to achieve reasonable performance, it is essential to use the resources provided by the cloud service provider (CSP) to store and share the data. Currently, various cloud mobile applications have been extensively used and in these applications, we can upload and share photos, videos, documents and other files.. In this context, data owners are allowed to choose either having their data files public or sharable with specific data users. Nevertheless, personal data files and other sensitive and valuable data files suffer from data privacy and security problems. This has been the concern for many data owners. The modern access control mechanisms provided by the CSP are neither adequate nor convenient. All the requirements of data owners are not being met. Principally , when data files are uploaded onto the cloud, the whereabouts of the data is not known ; data owner has no control or monitoring of his/her data and there are all possibilities of the CSPs searching out user data for their own commercial interests and/or other reasons. Subsequently, for sharing the encrypted data with specific users , password need to be sent to each data user which proves to be unwieldy.

To make things easier, the data owner can divide data users into diverse groups and provide password to the groups whom they want to share the data. But in this approach, apart from requiring a fine-grained privilege control, password administration is a big problem. Hence to address these challenges lightweight data sharing methods for mobile cloud computing have been suggested. In this work , an efficient lightweight data sharing scheme for mobile cloud computing which adopts the access control technology, CP-ABE is proposed. The experimental results prove the decrease in overhead for mobile users while sharing data in mobile cloud environments. The rest of this paper is organized as follows: Section II presents related works in mobile cloud data sharing and Section III gives the details of existing system and Section IV discusses the proposed system at length. Results and discussions appear in section V. Section 6 concludes our work with the mention of future work.

2. LITERATURE REVIEW:

In recent times, there have been sizeable studies on the subject of secured data access in the Cloud. In these researches, common considerations such as assumption of CSP to be truthful , encryption of all the sensitive data before uploading to the Cloud and achieving user authorization through encryption/decryption key distribution are common.

An access control method for Software as a Service (SaaS) model of cloud which is more and more used across enterprise precincts is presented by Qihua et al.[1]. Since there exists the chance of sensitive data being leaked to outsiders due to their employees' inadvertent mistakes on data sharing., a series of mechanisms are designed to provide defense in

depth against information leakage. Primarily enterprises are permitted to code their security rules as mandatory access control policies, so as to impose coarse-grained restrictions on their employees' discretionary sharing decisions. Secondly, an attribute-based recommender is designed that reduces errors in the choice of potential recipients. Thirdly, active prying of strange recipients providing defence before a file is shared.

Nowadays, using various applications, people can upload their pictures, films, documents and other files to the cloud and proportion those information with different people. In addition, CSPs offer data management functionality for data owners. Since personal data files are delicate , data proprietors are allowed to pick out whether to make their documents public or can be shared with specific information customers. Clearly, privacy of the non-public sensitive data is a huge challenge for many data owners. The present day privilege control gets right of entry to manipulate mechanisms provided by way of the CSP are either not sufficient or inconvenient.

Y.Liu et al. have proposed a "Security Aware Resource Allocation for Mobile Cloud Computing System"[2] . The request for accessing the Cloud resources from a mobiledevice is categorized according to the level of security requirement of a proposed resource allocation algorithm. As discussed in the research paper "Resource Allocation for Security Services in Mobile Cloud Computing" [3] which deals with mobile devices using cloud for searching, processing and mining, it is suggested to have two categories of Cloud security services, namely, Critical Security Services (CS) and Normal Security Services (NS).Though CS provides strong security protection, the cost of consumption of more resources is the drawback and CS users have to pay more than NS users.

The issue of privacy and the security of clients in the context of Mobile Cloud Computing has been discussed in the paper ,"An Efficient Model for Privacy and Security in Mobile Cloud Computing" [4]. Centralized Owner Model (COM) and Mobility Node Model (MNM) are the two models presented in this work to handle the issue of security by the user of trusted leader and proxy server respectively. A security framework is used for secure data storage in public cloud in "Efficient and Secure Data Storage Operations for Mobile Cloud Computing" [5]. Here a novel Privacy-Preserving Attribute- Based Encryption that ensures security of light-weighted devices by means of heavy encryption and decryption operation is used. Attribute-Based Data Storage (ABDS) structure is used to achieve minimized overhead of computation storage and communication.

The security of mobile users is at great risk owing to the browsing of malicious websites. In order to achieve security against such websites and to manage Man In The Middle attack, a secure web referral service called Secure Search Engine (SSE) for mobile devices is proposed byLe Xu et al. [6].

Itani W et al. have proposed a "Policy Based Security Channels for Protecting Network Communication in Mobile Cloud Computing" wherein a set of policy-driven security protocol is used for ensuring integrity and confidentiality of data [7]. The virtualized nature of cloud and trusted authority entities are used to afford energy efficient key management mechanism. Execution is done in a real cloud computing environment and studies on energy consumption and execution time are made..

3. EXISTING METHOD:

Normally, an encryption operation that requires one minute on a Personal Computer (PC) will need about thirty minutes to complete on a mobile device. Currently available solutions are really not good at tackling the user privilege-change problem since such an operation could result in high revocation costs. This is not applicable for mobile devices also. Evidently, there is no apt solution which may effectively solve the secure data sharing problem in mobile cloud.

The cloud servers could tamper or replace the delegated ciphertext and answer to a forged computing result with malicious intent. They might also cheat the eligible users by responding them that they are ineligible for the purpose of cost saving. Furthermore, during the encryption, the access policies might not be flexible enough too.
The concept of identity-based encryption (IBE) was introduced by Shamir [8] and conveniently substantiated by Boneh and Franklin[9]. IBE eliminates the necessity for providing a public key infrastructure (PKI).

Attribute-based encryption algorithm is derived from identity-based encryption. It embeds decryption rules in the encryption algorithm, which avoids frequent key distribution. Lai et al and Bethencourt et al proposed key-policy attribute-based encryption (KP-ABE) and ciphertext-policy attribute-based encryption (CP-ABE). In practical applications, CP-ABE has been extensively studied since it is similar to role-based access control (RBAC) scheme. In CP-ABE, the possession of an attribute key means that the key owner owns corresponding attribute, and attribute keys cannot be reclaimed once they are distributed. As a result, when a data user's attribute is revoked, ensuring data privacy becomes a difficult issue.

An attribute-based proxy re-encryption (ABPRE) scheme [10] to solve the problem of access control is discussed, However, in this scheme, fine-grained access control needs could not be satisfied when a user's attribute is revoked since all other users owning this attribute would lose that attribute all at once.

The following disadvantages are observed in these existing methods.

- No adequate mechanism for providing data security in the mobile cloud.

- High user authentication and revocation cost
- Inefficiency in checking the integrity of the data
- Once the client's secret key is exposed to cloud, the cloud can easily hide the data loss incidents for maintaining its reputation or dispose of the client's data rarely accessed for saving the storage space.

4. PROPOSED METHOD:

In the proposed approach, a Light weight Data Sharing Scheme (LDSS) has been used for mobile cloud computing environment and an algorithm called LDSS-CP supporting Attribute-Based Encryption (ABE) method to offer efficient access control over cipher text is designed. For encryption and decryption operations, proxy servers are used because computation- intensive operations in ABE are carried out on proxy servers. Thus ,computational overhead on client side mobile devices is reduced to a great extent. In LDSS-CP-ABE, in order to maintain data privacy, a version attribute is also added to the access tree structure. The decryption key format is modified with the intention that it can be sent to the proxy servers in a secure way. Efficient access of the data and increased performance at reduced cost are the main advantages of this proposed method.Ultimately, a data sharing model framework based on LDSS is implemented. The proposed LDSS , a framework of light weight data sharing system design is described below.

It has the four components, namely,Data Owner (DO), Data User (DU), Trust Authority (TA) and Cloud Service Provider(CSP).The architecture of proposed system is shown in fig.1.

A. Data Owner (DO):

DO can upload data to the mobile cloud and share it with his/her acquaintances. DO determines the access control policies on data files to assign attributes to a DU if he wants to access a particular data file. In this method, data files are encrypted with symmetric encryption mechanism, and symmetric key for data encryption is also encrypted using attribute based encryption. The access control policy is set in the ciphertext of symmetric key. Only a Data User obtaining attribute keys that satisfy the access control policy can decrypt the ciphertext and get back the symmetric key. Do send the majority of the data of the cloud. Since that cloud isn't tenable, the majority of the data must a chance to be encoded when it will be exchanged. The would characterize get with control methodology Similarly as entry control tree around the majority of the data records with consigning which qualities a DU ought will procure in the off chance that the necessities with getting on a particular majority of the data archive.

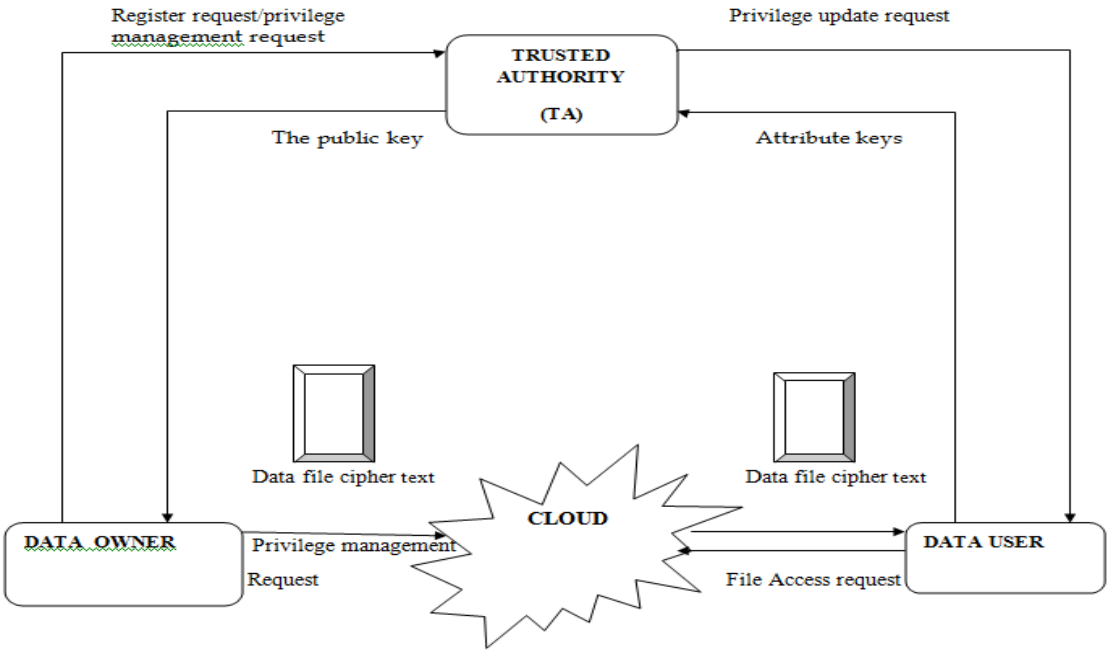

Fig.1 System Architecture of the proposed system

B. Data User (DU):

DU retrieves data from the mobile cloud. DU logins onto that skeleton Furthermore send an endorsement interest with ta. That Regard asks for incorporates characteristic keys (SK) which DU Likewise about notwithstanding need. Ta recognizes the Regard request What's more checks the interest Furthermore an item trademark magic (SK) for DU. DU sends an interest to data of the cloud. Cloud gets the interest and checks whether that DU meets that door need. DU gets that ciphertext, which incorporates ciphertext for the majority of the data documents and ciphertext of the

symmetric way. DU unscrambles those ciphertext of the symmetric magic for those help from claiming DSP. DU uses that symmetric enter should unscramble the ciphertext from claiming the majority of the data records.

C. Trusted Authority (TA):

To achieve LDSS accessible in a short time, a Trusted Authority (TA) is included in the system. TA is capable of bearing accessible and secret keys and dispersing acclaim keys to clients. It is responsible for generating attribute keys (Secret Keys) for DU and sending a Private Key to DO. DO can use the new Private Key to encrypt data files.

D. Cloud Service Provider(CSP):

CSP faithfully stores the data uploaded by DO. It truly executes the operations requested by DO though it may sneak a quick look over DO's data that has been stored in the cloud. In addition, CSP will undertake an initial access control and update data according to requests from users.

5. RESULTS AND DISCUSSIONS:

The proposed LDSS scheme developed for data sharing in mobile cloud is successfully implemented and the process of system initialization, user authorization and file sharing operations are done. And results show that the proposed approach has better performance compared to the existing ABE based access control schemes over ciphertext. The experiments reveal that LDSS can greatly reduce the overhead on the client side, since it brings in a minimal additional cost on the server side only. Thus the proposed approach proves helpful in implementing a pragmatic data sharing security scheme in mobile cloud. The screenshots taken during file upload selection, file upload after encryption and secure file download are shown in fig.2, fig.3 and fig.4 respectively.

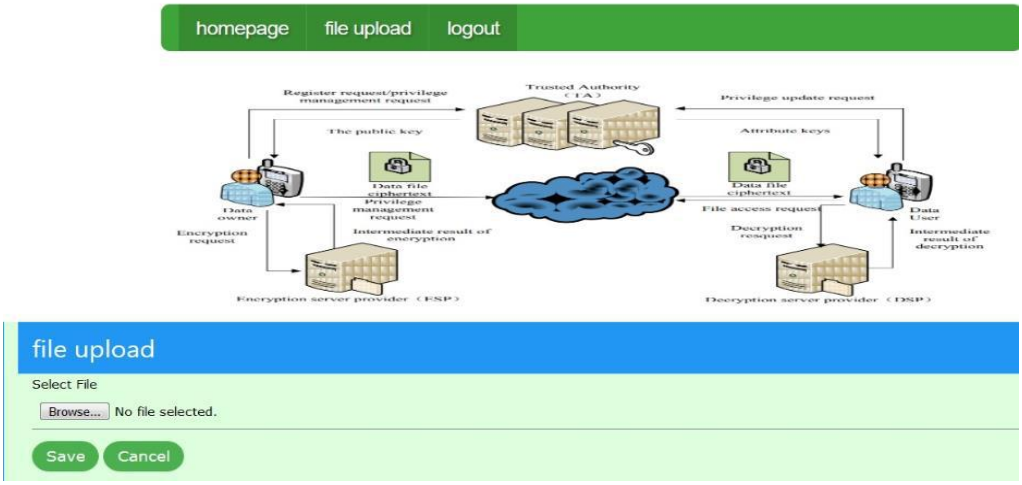

Fig.2 Screenshot showing file select option for file upload

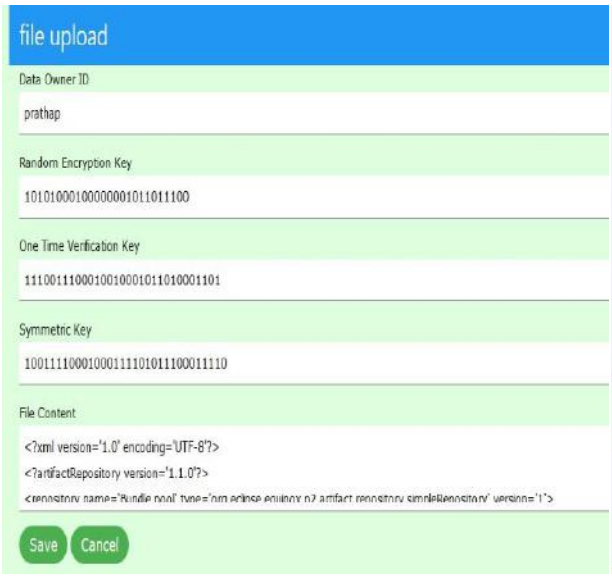

Fig.3 Screenshot showing keys generated for secure file upload

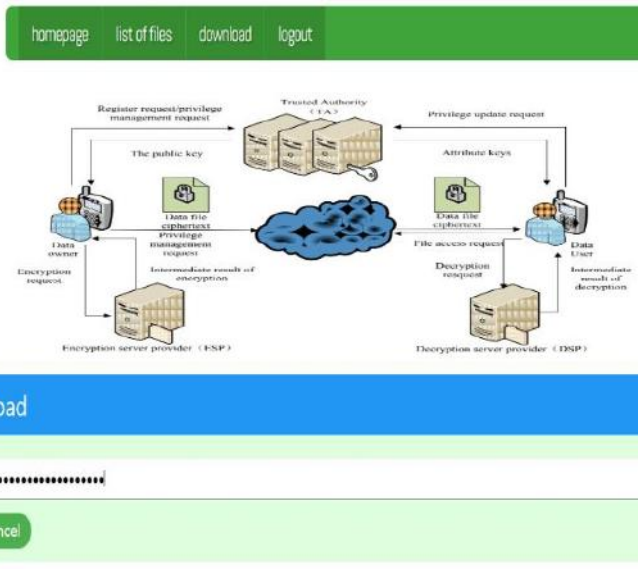

Fig.4 Screenshot showing secure file download

6. CONCLUSION:

In recent years, several studies on access control in cloud using attribute-based encryption algorithm (ABE) are carried out. However, traditional ABE is not suitable for mobile cloud because it is computationally intensive and moreover mobile devices have limited resources. In this paper, an efficient lightweight data sharing scheme (LDSS) that addresses the issue of limited resources of mobile devices is presented. It implements a novel encryption algorithm to transfer major computations from mobile devices onto proxy servers, thereby solving 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, study of ciphertext retrieval over existing data sharing schemes and new design approaches to ensure data integrity to further up the potential of mobile cloud may be considered.

REFERENCES:

1. 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.
2. Liu, Y, Lee, M.J., Security-Aware Resource Allocation for Mobile Cloud Computing Systems. Computer Communication and Networks (ICCCN), 24th International Conference on, 1-8 (2015).
3. Liang, H., Huang, D., Cai, L.X., Shen, X., Peng, D.: Resource Allocation for Security Services in Mobile Cloud Computing. IEEE INFOCOM 2011 Workshop on M2MCN, 191-195 (2011).
4. Ragini., Mehrotra, P., Venkatesan, S.: An Efficient Model for Privacy and Security in Mobile Cloud Computing. International Conference on Recent Trends in Information Technology, 1-6 (2014).
5. Zhibin Zhou , Dijiang Huang have proposed a paper “Efficient and Secure Data Storage Operations for Mobile Cloud Computing” - 8th international conference on network and service management (CNSM) , 2012.
6. Xu, L., Li, L., Nagaranjan, V., Huang, D., Tsai, W.T.: Secure Web Referral Services for Mobile Cloud Computing. IEEE Seventh International Symposium on Service-Oriented System Engineering, 584-593 (2013).
7. Itani, W., Kayssi, A., Chehab, A.: Policy Based Security Channels for Protecting Network Communication in Mobile Cloud Computing. Security and Cryptography (SECRYPT), Proceedings of the International Conference, 450-456 (2011).
8. Shamir, A.: Identity–based cryptosystems and signature schemes, Advances in Cryptography, Proceedings of Crypto’84 Lecture notes in Computer Science, 47{53}, (1984).
9. D. Boneh and M. K. Franklin, “Identity-based encryption from the Weil pairing,” in Proceedings of the Annual International Cryptology Conference (CRYPTO '01), vol. 2139 of Lecture Notes in Computer Science, pp. 213–229, Springer, 2001.
10. J. Li, X. Huang, J. Li, X. Chen and Y. Xiang, ”Securely Out-sourcing Attribute-based Encryption with Checkability,” in Proc. IEEE Transactions on Parallel and Distributed Systems,2013.