International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 5 Issue 1, November-December 2020 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

An Efficient and Safe Data Sharing Scheme for Mobile Cloud Computing

Abhishek. D[1], Dr. Lakshmi J. V. N[2]

[1]Master of Computer Application, [2]Assistant Professor,
[1,2]Department of Computer Application, Jain Deemed-to-be University, Bangalore, Karnataka, India

ABSTRACT

As the popularity of cloud computing is increasing, mobile devices at any time can store or retrieve personal information from anywhere. As a result, the issue of data protection in the mobile cloud is becoming increasingly severe and prevents more mobile cloud computing. There are important studies that have been carried out to strengthen the protection of the cloud. Most of them, however, are not applicable to mobile clouds, as mobile devices have restricted computing resources and power. In this paper, I propose a lightweight data sharing scheme (LDSS) for mobile cloud computing. It uses CP-ABE (Cipher text-Policy Attribute-Based Encryption), an access control technology used in basic cloud atmosphere, but changes the structure of access control tree to make it suitable for mobile cloud environments. LDSS moves a large portion of the computational rigorous access control tree transformation in CP-ABE (Cipher text-Policy Attribute-Based Encryption) from mobile devices to external proxy servers. Also, to reduce the user revocation cost, it introduces attribute description fields to implement lazy-revocation, which is a pointed issue in program based CP-ABE (Cipher text-Policy Attribute-Based Encryption) systems. The trial results show that LDSS can effectively lower the overhead on the mobile device side when users are sharing information in mobile cloud environments.

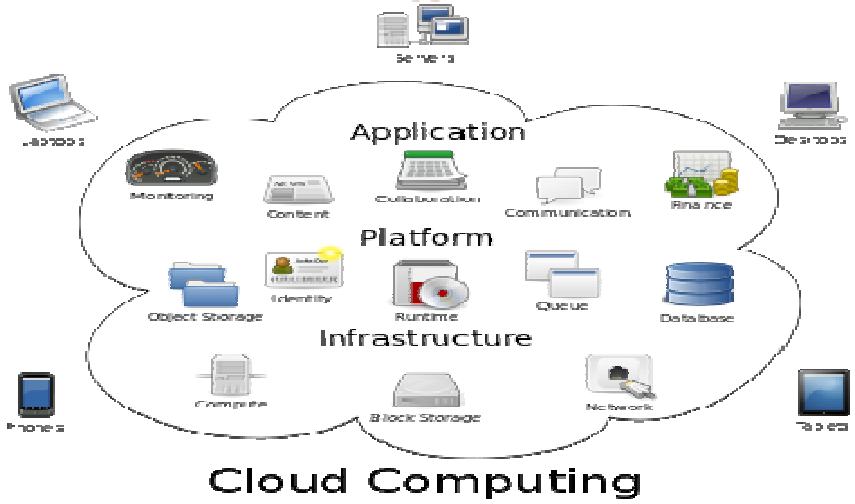
Keywords: *Cloud Computing, CP-ABE, Data Sharing, Access Control*

How to cite this paper: Abhishek. D | Dr. Lakshmi J. V. N "An Efficient and Safe Data Sharing Scheme for Mobile Cloud Computing" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-5 | Issue-1, December 2020, pp.312-315, URL: www.ijtsrd.com/papers/ijtsrd35909.pdf

IJTSRD35909

1. INTRODUCTION

Cloud computing is basically the use of computing resources that is both hardware and software that are delivered as a service over a network usually the Internet. The name arises from the common use of a cloud-shaped symbol as an concept for the complex set-up it contains in system diagrams. Cloud computing mentions 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 normally provide access to advanced software applications and high-end network of server computers.



1.1. Benefits of cloud computing:

A. **Low cost on technology infrastructure.** It allows us to access the data with initial spending. It is like a pay as you go model.

B. **Globalize our workforce for less cost or on cheap.** With basic internet connection people can access the cloud from anywhere.

C. **Streamline processes.** Get more work done in less time with less people.
D. **Reduce capital costs.** Don't need to spend huge amounts of money on hardware, software and licensing fees.
E. **Improve accessibility.** We can have access anytime, anywhere, making our lives easy
F. **Monitor the projects more effectively.** Stay within budget and ahead of completion cycle times.
G. **Higher personnel training not required.** It takes fewer people to do more work on a cloud, with a minimal learning curve on hardware and software issues.
H. **Minimize licensing new software.** Expand and grow without needing to buy high cost software licenses and programs.
I. **Improve flexibility.** We can change track without serious people or money issues at stake.

As we all know due to the limited storage of mobile devices the usage of cloud as increased widely because the cloud has more amount of storage and more resources which is basically provided by the cloud service provider. The concern for any person is that whenever he or she uploads files which can be images, documents etc there should be privacy and cannot be allowed to share it publically, although the management functionality is provided by the CSP still the personal information is important. First the control mechanism provided by csp is not sufficient because the criteria the user has will be more and more over the CSP itself can spy on the information. . So due to this problem the data owner will have to divide the data user into different users like who wants to share their password to particular group. Password management is a great issue for the privacy.

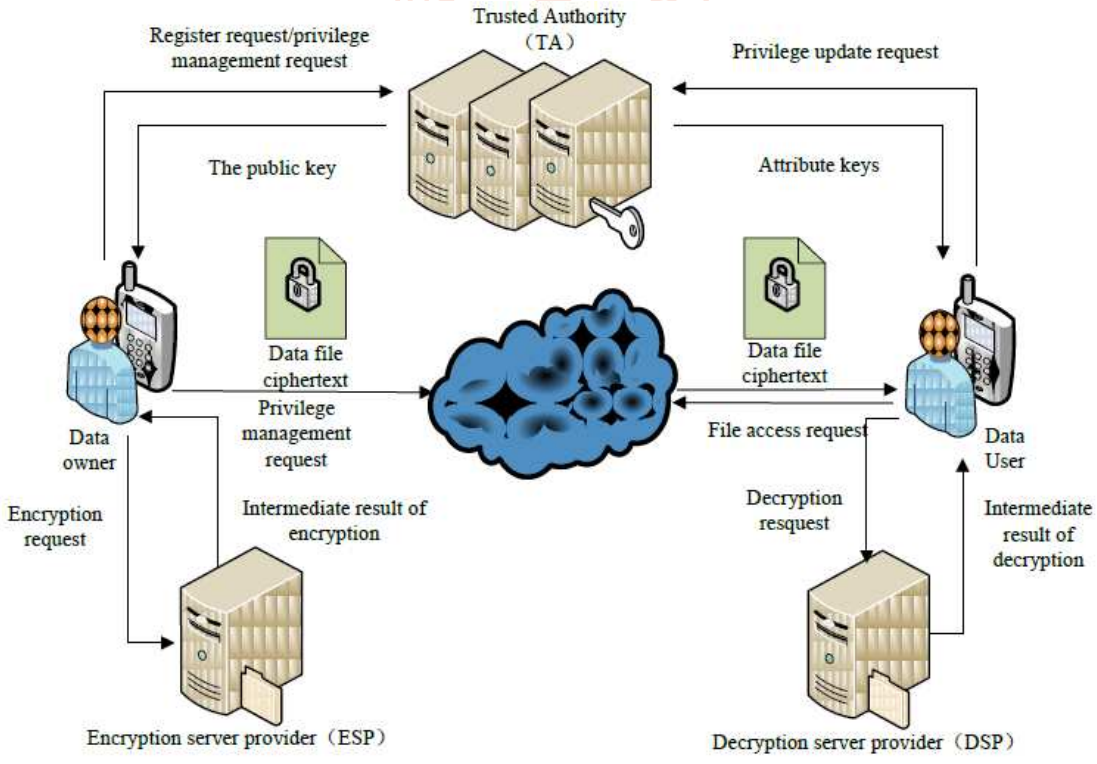
1.2. Advantages:

A. **COST:** We only pay for the resources we used.
B. **Security**: Cloud instances are secluded in the network from other instances for upgraded security.
C. **Performance:** Instances can be added instantly for added performance. Clients have access to the total resources of the Cloud's core hardware.
D. **Scalability:** Auto-deploy cloud instances when needed.
E. **Uptime:** Uses multiple servers for maximum redundancies. In case of server failure, instances can be automatically created on another server.
F. **Control:** We can login from anywhere. Server snapshot and a software library lets us deploy custom instances.
G. **Traffic:** Deals traffic control with fast implementation of additional instances to lower the load.[1],[2],[3],[4],[5].

2. Cipher text-policy Attribute-Based Encryption Scheme

CP-ABE (Cipher text-Policy Attribute-Based Encryption) with hidden access management policy allows information owners to share their encrypted data mistreatment cloud storage with approved users whereas keeping the access control policies blinded [6], [7]. However, a process to stop users from achieving sequential access to an information owner's sure range of knowledge objects, that gift a conflict of interest or whose combination there from is sensitive has nevertheless to be studied. during this paper, I tend to analyze the underlying relations among these specific data objects, introduce the conception of the sensitive data set constraint, and propose a CP-ABE access control theme with hidden attributes for the sensitive data set constraint. This theme incorporates extensible, partly hidden constraint policy. In this scheme, thanks to the separation of duty principle, the duties of implementing the access management policy and therefore the constraint policy are divided into two freelance entities to reinforce security. The hidden constraint policy provides flexibility in this the data owner will partially amend the sensitive data set constraint structure when the system has been set up. [8],[9],[10],[11].

3. System Architecture



4. Existing System Disadvantages

A. Sensitive data or personal data is a big concern for many data owners.
B. The state-of-the-art privilege access control mechanisms provided by the CSP are is simply not enough.
C. The data owners have some requirements and it doesn't meet them.
D. They occupy huge amount of space and computation resources, which are not available for mobile devices
E. Present solutions doesn't solve the user privilege change problem very well.
F. Such an operation could result in very high revocation cost and it will not be applicable for mobile devices .

5. Problem Statement

To ensure security in lightweight manner resource mobile devices in cloud environment and to have light weight revocation policy. The encrypted and decrypted information will be secured using secret key. The sharing of the file will be among the right users who have the access privileges. There should also have the opportunity to lower the overhead of the cryptographic standard algorithm and study the security systems with low overhead.

6. Proposed Approach

The proposed approach will be using a Lightweight Data Sharing Scheme (LDSS) for mobile cloud computing environment. The main contributions of LDSS are as follows:[12],[13],[14],[15],[16],[17].

It will be using the designed algorithm called LDSS-CP-ABE based Attribute-based Encryption (AES) used for access control over cipher text well. Here the proxy servers will be used for encryption and decryption methods. ABE is used for the computational severe operations for conducting on the proxy servers, which help in lowering the computational load on the client side of the mobile devices. There is also management of the data privacy using LDSS-CPABE. The updated version of decryption key is sent in safe manner to the proxy servers. The lazy encryption and decryption field of attributes are introduced to clear out the user's revocation problem. At last, to have a information sharing outline prototype based on LDSS.

7. Methodology

The LDSS framework for lightweight data sharing scheme in mobile cloud has the following three components, First one is the Data Owner (DO) and the Data Owner is used to upload the information to the mobile cloud and share it with different users. Data owner determines the access control policies. Second one is Data User (DU), the Data User is used to retrieve information from the mobile cloud. Third one is the Trust Authority (TA),Trust Authority is responsible for generating and sharing attribute keys.

8. Conclusion

In past years, many studies on access control in cloud are based on attribute-based encryption algorithm (ABE).But, traditional ABE is not appropriate for mobile cloud because it is computationally severe and mobile devices only have inadequate resources. In this paper, I 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, so it can solve the safe data sharing problem in mobile cloud. The output results show that LDSS can make sure data privacy in mobile cloud and lower the overhead on users' side in mobile cloud. In the future work, I will design new approaches to ensure data integrity. To further tap the potential of mobile cloud, we will also study how to do cipher text retrieval over existing data sharing schemes.

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

[11] Yu S., Wang C., Ren K., Lou W. Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing. INFOCOM 2010, pp. 534-542, 2010

[12] Kan Yang, Xiaohua Jia, Kui Ren, Bo Zhang, Ruitao Xie: DACMACS: Effective Data Access Control for Multiauthority Cloud Storage Systems. IEEE Transactions on Information Forensics and Security, Vol. 8, No. 11, pp.1790-1801, 2013.

[13] Stehlé D, Steinfeld R. Faster fully homomorphic encryption. In: Proceedings of 16th International Conference on the Theory and Application of Cryptology and Information Security. Singapore: Springer press, pp.377-394, 2010.

[14] Junzuo Lai, Robert H. Deng, Yingjiu Li ,et al. Fully secure key policy attribute-based encryption with constant-size cipher texts and fast decryption. In: Proceedings of the 9th ACM symposium on Information, Computer and Communications Security (ASIACCS), pp. 239-248, Jun. 2014.

[15] Bethencourt J, Sahai A, Waters B. Ciphertext-policy attribute based encryption in: Proceedings of the 2007 IEEE Symposium on Security and Privacy (SP). Washington, USA: IEEE Computer Society, pp. 321-334, 2007.

[16] Liang Xiaohui, Cao Zhenfu, Lin Huang, et al. Attribute based proxy re-encryption with delegating capabilities. In: Proceedings of the 4th International Symposium on Information, Computer and Communications Security. New York, NY, USA: ACM press, pp. 276-286, 2009.

[17] Pirretti M, Traynor P, McDaniel P, et al. Secure attribute-based systems. in: Proceedings of the 13th ACM Conference on Computer and Communications Security. New York, USA: ACM press, pp. 99-112, 2006.