ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 11, November 2017

Storage Outsourcing with Secure Accessibility in Mobile Cloud Computing by Using LDSS

Puja Pingale[1], Dipanjali Gaikwad[1], Ashwini Bhapkar[1], Rutuja Pharande[1], Monika Waghmare[2]

U.G. Student, Department of Computer Engineering, Someshwar Engineering College, Someshwarnagar, Maharashtra, India[1]

Assistant Professor, Department of Computer Engineering, Someshwar Engineering College, Someshwarnagar, Maharashtra, India[2]

ABSTRACT: Mobile device has limited storage and limited computing resources so data can be stored on mobile cloud computing .Any user can upload data on that cloud also anyone can access that data, so there is security issue related to that data so, we need to provide security to that data to prevent from unauthorized user. Now a days, the cloud computing becomes more popular but the security is not provided in efficient manner. The issues related to security is increases day by day. Some algorithms are designed to provide security to cloud computing but those are not efficient for mobile cloud computing so we design LDSS-CP-ABE algorithm for provide security to the mobile cloud computing. LDSS migrates major computational overhead from mobile client side devices using proxy servers. Also we can use lazy re-encryption method which can reduce time consuming process. Lightweight secure data sharing scheme can reduce the computational overhead on the client side mobile device when users are sharing their data on mobile cloud . Also we use the AES (Advance Standard Encryption) algorithm for data encryption and decryption purpose.

KEYWORDS: Mobile Cloud Computing, Data Encryption, Access control, User revocation.

I.INTRODUCTION

In cloud computing huge amount of data store on cloud by using different smart devices or computer.Cloud computing means, storage of data and application on remote server and accessing them via internet rather than saving and installing them on your personal devices and computers. As the mobile devices has limited storage space we use the mobile cloud computing for storing data. Mobile cloud computing is nothing but mobile computing + cloud computing.

Day by day popularity and use of mobile devices are increased rapidly, so people can use new era to store data on cloud and store/retrieve that data by using mobile devices. As the mobile device have limited computation power and storage the cloud contain huge amount of resources so it is essential to use the cloud resources provided by cloud service provider(CSP) to store and share data.

Now a days many application of cloud mobile have widely used. People (Data Owner) can share data. For example: text, video, audio on mobile cloud and people (Data User) who need to data can retrieve it. As data owner decided the data which shared is public or private. Clearly for data owner sensitive data privacy is major concern. CSP (Cloud Service Provider) cannot meet all requirement of data owner. First when data owner needs to store data on cloud, data owner can divide number of users into group and share the password to that group which is data owner wants to send but in this approach management of password is big issue.

Different algorithm are invented or present for providing security to cloud but it is not suitable for mobile cloud computing, so use LDSS for providing security to data stored on mobile cloud. The main benefit of mobile cloud computing and our proposed system is to reduced computational overhead on client side mobile device and provide security to data on mobile cloud.

Apparently, personal sensitive data should be encrypted before uploaded onto the cloud so that the data is secure against the Cloud Service Provider. The data encryption brings new problems. How to provide access control

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 11, November 2017

mechanism on cipher text decryption so that only the authorized users can access the plaintext data is challenging. In addition, system offer data owner's effective user privilege management capability, so they can grant data access privileges easily on the data users. 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).

Finally, we implement a data sharing prototype framework based on LDSS and also used the AES(Advance Encryption Standard) algorithm for purpose of encryption of data which are uploaded on mobile cloud computing.

II .LITERATURE SURVEY

1] A Lightweight Secure Data Sharing Scheme for Mobile Cloud Computing.
Authors: ChenglinShen, Heng He
Description: This paper describes that Mobile device has limited storage and limited computing resources so data can be stored on mobile cloud computing .Any user can upload data on that cloud also anyone can access that data, so there is security issue related to that data so, it need to provide security to that data to prevent from unauthorized user. In this paper, design LDSS-CP-ABE algorithm for provide security to the mobile cloud computing.

2]How to build a trusted database system on untrusted storage.
Authors: Maheshwari U, Vingralek R, Shapiro W.
Description: In this Paper, It can identify the problem of ensuring trustworthiness of data at an untrusted server in the presence of transactional updates that run directly on the database, and develop the first solutions to this problem.

3]Achieving Usable and Privacy-assured Similarity Search over Outsourced Cloud Data.
Authors: Cong Wang, KuiRen, Shucheng Yu
Description: In this paper, It investigate the problem of secure and efficient similarity search over outsourced cloud data.In this any user can upload data on cloud and also achieves the usable and privacy assured similarity search over outsourced cloud data.

4]A flexible mechanism for access control enforcement management in DaaS. In: Proceedings of IEEE International Conference on Cloud Computing.
Authors: Tian X X, Wang X L, Zhou A Y.
Description: In this paper, First present an approach to implement the flexible access control enforcement management by applying a DSP re-encryption mechanism also this re-encryption mechanism is used repeatedly.

5]Hybrid attribute- and re-encryption-based key management for secure and scalable mobile applications in clouds.
Authors:P. K. Tysowski and M. A.Hasan
Description:cloud-based data are increasingly accessed by resource-constrained mobile devices for which the processing cost must be minimized.In this paper, re-encryption mechanism is performed optionally.

III.METHODS AND TECHNIQUES USED

1) LDSS (Lightweight secure data sharing scheme):

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 provide security to the lightweight data sharing scheme on mobile cloud. In LDSS it uses attribute based encryption which has another two subparts that is:

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

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 11, November 2017

In our System, We use the CP-ABE (Cipher Policy –Attribute based Encryption). CP-ABE provide the encryption of data mechanism.

2) AES(Advanced Encryption Standard):

i. To review the overall structure of AES and to focus particularly on the four steps used in each round of AES: (1) byte substitution, (2) shift rows, (3) mix columns, and (4) add round key

ii. AES is a block cipher with a block length of 128 bits.

iii. AES allows for three different key lengths: 128, 192, or 256 bits. Most of our discussion will assume that the key length is 128 bits. Encryption consists of the 10 rounds of processing for 128-bit keys, 12 rounds of processing for 192-bit keys, and 14 rounds of processing for 256-bit keys.

IV. PROPOSED SYSTEM

In Proposed system, we describe the LDSS system design. First, we refer the overview of LDSS(Lightweight secure data sharing scheme), and then we present LDSS-CP-ABE algorithm and system operations.

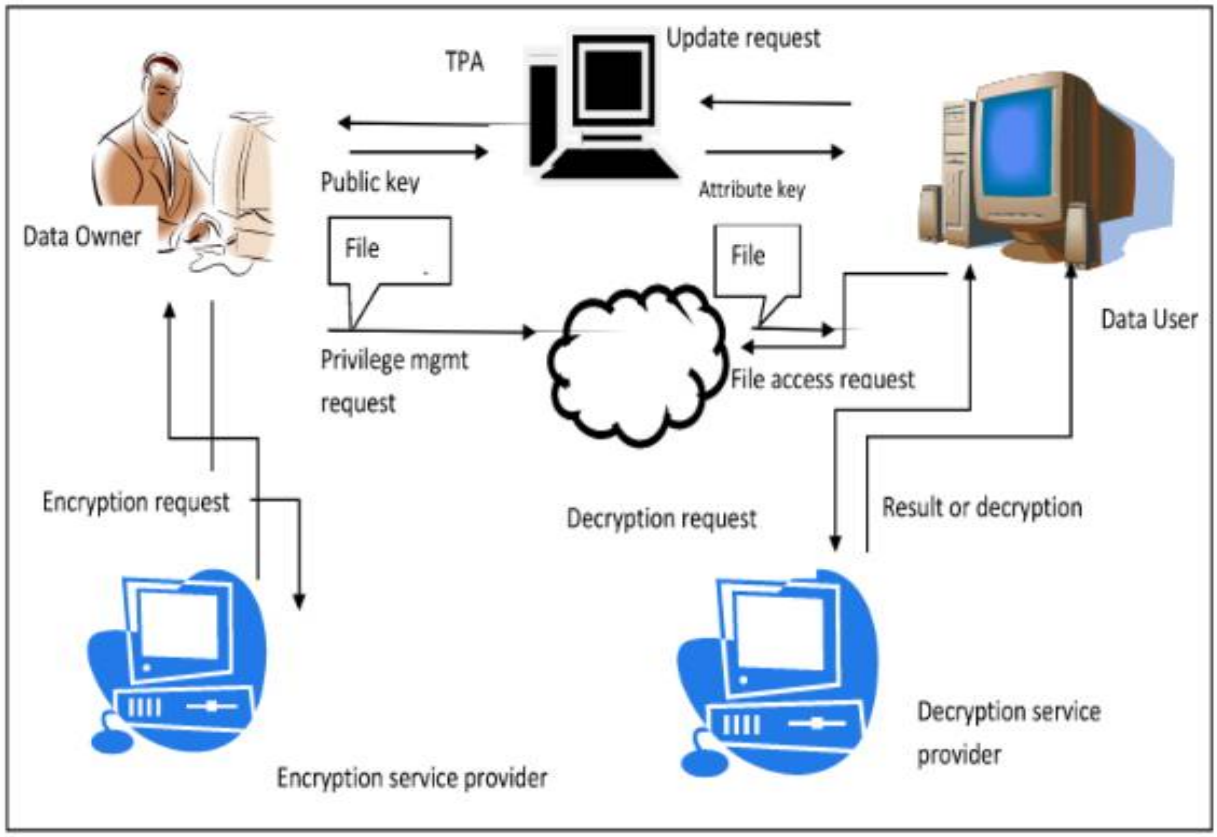

Fig. A lightweight data-sharing scheme (LDSS) framework

In Proposed system, We develop the Architecture of LDSS by using Following six component:

(1) Data Owner (DO)
(2) Data User (DU)
(3) Trust Authority (TA)

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 11, November 2017

(4) Encryption Service Provider (ESP)
(5) Decryption Service Provider (DSP)
(6) Cloud Service Provider (CSP)

Firstly DO send data to the cloud. Since the cloud is not credible, data has to be encrypted before it is uploaded. The DO defines access control policy in the form of access control tree which policies are such as read the data, write the data. Data files to assign which attributes a DU should obtain if he wants to access a certain data file. In LDSS, data files are all encrypted using symmetric encryption mechanism, and the symmetric key for data encryption is also encrypted using attribute based encryption (ABE).

In our proposed system, data owner, TPA is present on equal level of authority. Data owner firstly should register or login on website then as it nothing but work like aCSP (cloud service provider) then he can upload his own files on cloud in encrypted format. Data user can register or login on website for access for files ,After login of data user on cloud server then request goes to the data owner then data owner decide the approve of files access to user or not. Data user has acknowledgment from data owner if he approves the request of data user.

Third party authorization is used to monitories the data owners activities also it can check the integrity, durability of files which are uploaded by data owner on mobile cloud computing. Trusted authority (TA) also generates the report for data owner. While requesting of data user of some kind of data from cloud, data owner select the role for data user and also after approval of users request he send the public key to data user through the email then data user can retrieve the information from cloud by entering the key on website but this information it in the form of encryption so to decrypt that data .Data owner provide the private key to data user from mail. Then by using this key Data User can decrypt that data.

To relieve the overhead on the client side mobile devices, encryption service provider (ESP) and decryption service provider (DSP) are used. Both the encryption service provider and the decryption service provider are also semi-trusted. We modify the traditional CP-ABE algorithm and design an LDSS-CP-ABE algorithm to ensure the data privacy when outsourcing computational tasks to ESP and DSP, also we used the AES (Advanced Encryption Standard) algorithm to encrypt and decrypt the overall data which are uploaded on mobile cloud by data owner.

V. CONCLUSION AND FUTURE WORK

Conclusion:

In recent year, Attribute Based Encryption (ABE) algorithm used for cloud but mobile device has limited resource and Attribute Based Encryption is computationally intensive, so ABE is not suitable for mobile devices. In this paper we propose LDSS for secure sharing of data on mobile cloud, Also we can use Advance Encryption Standard (AES) for perform encryption and decryption of data. Proposed system reduces computational overhead on mobile device. We use proxy servers for encryption and decryption also reduces time complexity by using lazy re-encryption method. Also we refer Third Party Authorization (TPA) for authentication purpose .By using TPA we can check integrity, durability, consistency of related files which are uploaded by data owner.

Future Scope:

1. Battery Saving:
   In future work, we will design new approach to saving the Battery of mobile devices.

REFERENCES

[1] ChenglinShen, Heng He. “A Lightweight Secure Data Sharing Scheme for MobileCloud Computing”. Ruixuan Li, Member, IEEE 2016.
[2] 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.
[3] 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.
[4] 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.
[5] 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.
[6] 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.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 11, November 2017

[7] 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.
[8] Kan Yang, XiaohuaJia, KuiRen: "Attribute-based fine-grained access control with efficient revocation in cloud storage systems". ASIACCS 2013, pp. 523-528, 2013.
[9] Crampton J, Martin K, Wild P. "On key assignment for hierarchical access control. in: Computer Security Foundations Workshop". IEEE press, pp. 14-111, 2006.
[10] 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. 350364
[11] Cong Wang, KuiRen, Shucheng Yu, and KarthikMahendraRajeUrs."Achieving Usable and Privacy-assured Similarity Search over Outsourced Cloud Data". IEEE INFOCOM 2012, Orlando, Florida, March 25-30, 2012
[12] 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
[13] Kan Yang, XiaohuaJia, KuiRen, Bo Zhang, RuitaoXie: "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.
[14] 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.
[15] Junzuo Lai, Robert H. Deng ,Yingjiu Li ,et al. "Fully secure keypolicy attribute-based encryption with constant-size ciphertexts and fast decryption. In: Proceedings of the 9th ACM symposium on Information, Computer and Communications Security" (ASIACCS), pp. 239-248, Jun. 2014.