ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 7, Special Issue 6, May 2018

2nd National Conference on "RECENT TRENDS IN COMPUTER SCIENCE & INFORMATION TECHNOLOGY (RTCSIT'18)"

13th-14th March 2018

Organized by

Departments of Computer Science & Information Science Engineering, Sri Krishna Institute of Technology, Bangalore, India

An Efficient Lightweight Secure Data Sharing Scheme for Mobile Cloud Computing

Princy P. James[1], Renuka Ajay Sonone[2], Naveen Ghorpade[3], Reddy Kumar V[4]

U.G. Student, Department of CSE, Sri Krishna Institute of Technology, Chikkabanavara, Bangalore India

U.G. Student, Department of CSE, Sri Krishna Institute of Technology, Chikkabanavara, Bangalore, India

Assistant Professor, Department of CSE, Sri Krishna Institute of Technology, Chikkabanavara, Bangalore, India

Programmer, Department of ISE, Bangalore, India

ABSTRACT: Cloud storage is a simple and scalable way to store, access, and share data over the Internet. Consequently, the data security problem in mobile cloud becomes more and more severe and prevents further development of mobile cloud. There are essential studies that have been conducted to improve the cloud security. However, most of them are not relevant for mobile cloud since mobile devices only have finite computing resources and power. Solutions with low computational expenses are in need for mobile cloud applications. In this paper, we present a lightweight data sharing scheme (LDSS) for mobile cloud computing. It adopts CP-ABE (Attribute Based Encryption), an access control technology used in normal cloud environment, but changes the structure of access control tree to make it acceptable for mobile cloud environments. Furthermore, to reduce the user revocation cost, it introduces attribute description fields to implement lazy-revocation, which is a delicate issue in program based CP-ABE systems. The experimental results show that LDSS can effectively reduce the overhead on the mobile device side when users are sharing data in mobile cloud environments.

KEYWORDS: mobile cloud computing, data encryption, access control, user revocation

I. INTRODUCTION

The popularity of smart mobile devices and development of cloud computing, people are slowly getting familiar 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. Usually, mobile devices only have limited storage space and computing power. On the opposite side, the cloud has huge amount of resources. In such a framework, to achieve theadequate performance, it is important to use the resources provided by the cloud service provider (CSP) to store and share the data.Nowadays, various cloud mobile applications have been widely used. In these applications,data owners can upload their photos, videos, documents and other files to the cloud and share these data with data users they like to share. CSPs also provide data management functionality for data owners. Since personal data files are sensitive, data owners are allowed to choose whether to make their data files public or can only be shared with specific data users. Clearly, data privacy of the personal sensitive data is a big concern for many data owners. The state-of-the-art privilege management/access control mechanisms provided by the CSP are either not sufficient or not very convenient. They cannot meet all the requirements of the data owners.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.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 7, Special Issue 6, May 2018

2nd National Conference on "RECENT TRENDS IN COMPUTER SCIENCE & INFORMATION TECHNOLOGY (RTCSIT'18)"

13th-14th March 2018

Organized by

Departments of Computer Science & Information Science Engineering, Sri Krishna Institute of Technology, Bangalore, India

II. LITERATURE SURVEY

1. A Lightweight Secure Data Sharing Scheme for Mobile Cloud Computing. Authors:Chenglin Shen, 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.HasanDescription: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.

IV. PROPOSED SYSTEM

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

(1) Data Owner (DO): DO uploads data to the mobile cloud and share it with friends. DO determines the access control policies.
(2) Data User (DU): DU retrieves data from the mobile cloud.
(3) Trust Authority (TA): TA is responsible for generating and distributing attribute keys.
(4) Encryption Service Provider (ESP): ESP provides data encryption operations for DO.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 7, Special Issue 6, May 2018

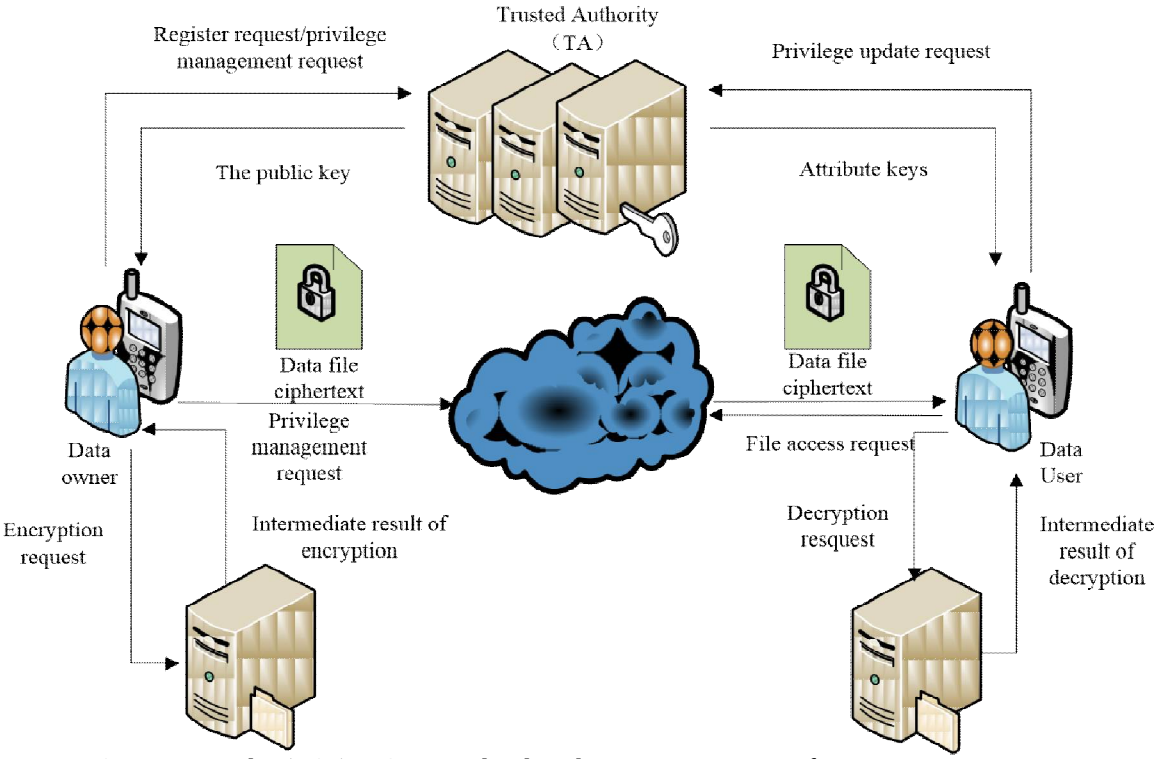
2nd National Conference on "RECENT TRENDS IN COMPUTER SCIENCE & INFORMATION TECHNOLOGY (RTCSIT'18)"

13th-14th March 2018

Organized by

Departments of Computer Science & Information Science Engineering, Sri Krishna Institute of Technology, Bangalore, India

fig. The Proposed System Architecture



(5) Decryption Service Provider (DSP): DSP provides data decryption operations for DU.
(6) Cloud Service Provider (CSP): CSP stores the data for DO. It faithfully executes the operations requested by DO, while it may peek over data that DO has stored in the cloud.

1. Text Encryption and Decryption

User encrypted the plain text to encrypted format and uploaded to the cloud. The encryption is done by using a password. Only using this password only anyone can decrypt the text. The user upload the password also include with encrypted data. The trusted authority id responsible for passing the password to the requested user

2. Image Encryption and decryption

Like the same as the image encryption is also done. And the encrypted images and password will also be uploaded to the cloud. The trusted authority id responsible for passing the password to the requested user.

3. Text request

Any user can view the file uploaded in the server. All the files are in encrypted format. User can't view the files without know the password. For view the file first user need to request the password to Trusted Authority. TheAuthority check the user and provide the password for valid user.

4. Image request

Image request is also same as the Text Request. The list of images can view in the application. But user can only view the images after getting the password from trusted authority.

5. View Encrypted Data

The user uploaded encrypted data can be view in the server side. The trusted authority act as server they have the responsibility to provide password for the requested user.

6. View user request

After user view the encrypted data they can request the password for encrypted data. This user request can be view in the Trusted authority.

7. Provide password

After view the request Trusted authority validating the user and if the user is valid the Trusted authority provide password for the requested file via email. Using this password user can decrypt the file

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 7, Special Issue 6, May 2018

2nd National Conference on "RECENT TRENDS IN COMPUTER SCIENCE & INFORMATION TECHNOLOGY (RTCSIT'18)"

13th-14th March 2018

Organized by

Departments of Computer Science & Information Science Engineering, Sri Krishna Institute of Technology, Bangalore, India

V. CONCLUSION

This paper has presented a novel secure information management architecture and implementation. We propose LDSS to address this issue. It shows a novel LDSS-CP-ABE calculation to move noteworthy estimation overhead from phones onto go-between servers, thus it can deal with the secured data sharing issue in flexible cloud. 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. 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, durability, consistency of related files which are uploaded by data owner.

VI. ACKNOWLEDGEMENT

This work is supported by Chinese National Scholarship Fund and Chinese National High Technology Research and Development Program 863 under Grant No. 2012AA121604, as well as the US National Science Foundation (NSF) under grant CNS-1065444.

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, HongxiaJin. "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.
[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, XiaohuaJia, KuiRen: 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. 350364
[10] 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
[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, 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.
[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 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.
[15] Bethencourt J, Sahai A, Waters B. Ciphertext-policy attributeIEEE Transactions on Cloud Computing, January 2017 based encryption. in: Proceedings of the 2007 IEEE Symposium on Security and Privacy (SP). Washington, USA: IEEE Computer Society, pp. 321-334, 2007.

.

.