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. 6, Issue 5, May 2018

Secure Data Sharing for Mobile Cloud Using A Trivial Sharing Method

Mukunthan B [1], M G Dinesh[2]

PG Student, Department of Computer Science and Engineering, Easa college of Engineering and Technology, Coimbatore, India[1]

Assistant Professor, Computer Science and Engineering, Easa college of Engineering and Technology, Coimbatore, India[2]

ABSTRACT: Mobile device has restricted data storing capacity and constrained computing resources, because of that the data can be put away on mobile cloud processing to make it more accessible .Any client can transfer data on that cloud meanwhile anybody can get in to that data also. There is a security issue identified with that data .To provide security to that data in order to protect from unapproved client. Even, the cloud computing turns out to be better level the security isn't given in productive way. The issues identified with security got expanded day by day. Algorithms are intended to give security to cloud computing however those are not proficient for portable cloud computing. An algorithm called TDSS-CP-ABE algorithm for give security to the mobile cloud computing is introduced here. TDSS removes major computational overhead from portable customer side devices utilizing intermediate servers. Likewise re-encryption technique which can lessen tedious process. Trivial secure data sharing plan can decrease the computational overhead on the customer side mobile device when clients are sharing their data on portable cloud. Likewise we utilize the AES (Advance Standard Encryption) algorithm for data encryption.

KEYWORDS*:* Mobile Cloud Computing, Data Encryption, Data Decryption, Security, Data sharing, portable cloud, Standard encryption.

I. INTRODUCTION

Mobile Cloud Computing (MCC) is the combination of Two Computing Technologies: 1) Mobile 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 Cloud computing refers to both the applications delivered as services over the Internet and the hardware and systems software in the datacentres that provide those services" Mobile Cloud Computing is defines as it provide Infrastructure where both computationally intensive and secure data storage of mobile devices are offloaded or migrate to cloud servers. A service that allows resource constrained mobile users to adaptively adjust processing and storage capabilities by transparently partitioning and offloading the computationally intensive and storage demanding jobs on traditional cloud resources by providing ubiquitous wireless access

Secure data sharing in these application scenarios pushes the development and usage of cryptographic schemes in supporting access control. Among these cryptographic schemes, Ciphertext Policy Attribute-Based Encryption (CP-ABE) is regarded as one of the most expressive technologies and is a natural fit for attribute-based access control in secure data sharing. In CP-ABE, each user is entitled a set of attributes based on his/her role or identity, which are embedded into the private key by the trusted authority that is responsible for system setup and key generation/distribution. A data owner enforces an access policy over the shared data directly by encrypting the data with the access structure extracted from the access policy. Instead of by the server, the access checking is done "inside the cryptography", where only data users with eligible attributes (i.e., satisfying the access structure) could decrypt the ciphertext. Different from identity-based and role based cryptographic schemes, the public key and ciphertext size of CP-ABE are not related with the number of data users and no interactions among data owners and data users are needed

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. 6, Issue 5, May 2018

Moreover, CP-ABE is resistant against collusion attacks from unauthorized users. All these nice properties make CP-ABE very suitable for implementing fine-grained access control for secure data sharing in cloud computing where the cloud servers can't be fully trusted or mobile ad hoc networks (MANET), Peer-to-Peer (P2P) networks, and the recently proposed information centric networks (ICN) where no centralized server exists after system deployment. As promising as it is, multiple users might share common attributes with each other, thus making user management, especially user revocation extremely difficult to handle when applying state-of-the-art CP-ABE schemes to practical applications.

Previous researches define the revocation problem as attribute-based revocation. The basic idea of attribute based revocation is to cease certain access privileges of users from the perspective of key generation. In particular, it is a key re-distribution process. Whenever an attribute revocation occurs, the trusted authority generates some secret information for non-revoked users to update their private key. Since the revoked user doesn't have the secret updating information, the components of his/her private key corresponding to the revoked attributes will not work anymore when used to decrypt newly generated ciphertexts, thus achieving the goal of ceasing certain users' access privilege(s).

Although attribute-based revocation is a feasible solution to the user revocation problem in CP-ABE, it suffers the following deficiencies when applied in practice. First, trusted authority has to be online all the time to deal with each revocation and keeps a mapping between each attribute and the corresponding list of the non-revoked users in order to distribute secret information. Once the authority is down, the user revocation functionality cannot be implemented any more. Moreover, in some application scenarios, such as MANET, P2P networks, once the system is set up, there would be no communication between the trusted authority and the nodes in the network except for system re-setup. Second, non-revoked users owning common attributes with the revoked user(s) have to update their private keys, which will bring in great computation and communication overheads when the revoked users have a great number of attributes, the number of the non-revoked users sharing common attributes with the revoked users is big, or user revocation frequency is high. The reason leading to the aforementioned deficiencies is that revocation is performed from the perspective of key generation. To this end, we propose a new scheme HIR-CP-ABE, which implements user revocation from the perceptive of encryption. Different from previous attribute-based approaches, HIR-CP-ABE supports identity-based revocation. In the key generation phase, on the one hand attributes are allocated to users as in state-of-the-art CP-ABE schemes, on the other hand a unique identity (ID) is assigned to each user. That is, both attributes and the ID are embedded into a user's private key.

II. RELATED WORK

Attribute-based encryption (ABE) is proposed by Sahai and Waters. Attribute-based encryption (ABE) is a moderately late approach that re-evaluates the idea of public key cryptography. Attribute-based encryption is also referred to as ABE is a sort of public-key encryption wherein the secret key of a person and the cipher-text is established upon attributes[8]. In an ABE, a person's keys and cipher-texts are labeled with units of descriptive attributes and a symmetric key can decrypt a selected cipher-text only if there's a match between the attributes of the cipher-text and the person's key[4]. It reduces the quantity of key used and hence makes encryption and decryption technique faster

III. PROBLEM DEFINITION

Mobile device has restricted capacity and constrained computing resources so data can be put away on mobile cloud processing. Any client can transfer data on that cloud and additionally anybody can get to that data. A security issue is identified with that data retrieving process. Therefore, a security mechanism need to be implemented in order to achieve high level data security during the data sharing process.

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. 6, Issue 5, May 2018

IV. EXISTING SYSTEM

In the existing system, a lightweight data sharing scheme (LDSS) has been used for mobile cloud computing. It adopts CP-ABE, an access control technology used in normal cloud environment, it changes the structure of access control tree to make it suitable for mobile cloud environments. LDSS moves a large portion of the computational intensive access control tree transformation in CP-ABE from mobile devices to external proxy servers. Furthermore, to reduce the user revocation cost, it introduces attribute description fields to implement lazy-revocation, which is a thorny issue in program based CP-ABE systems. Thus this solutions don't solve the user privilege change problem very well. Such an operation could result in very high revocation cost. This is not applicable for mobile devices as well. Clearly, there is no proper solution which can effectively solve the secure data sharing problem in 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.

Disadvantages of Existing System

- There is no proper mechanism for providing the security for data that is presented in the mobile cloud.
- User authentication and Revocation cost will be high**.**
- 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.
- It cannot meet all the requirements of data owners.
- It consume large amount of storage and computation resources, which are not available for mobile devices
- Current solutions don't solve the user privilege change problem very well. Such an operation could result in very high revocation cost. This is not applicable for mobile devices as well. Clearly, there is no proper solution which can effectively solve the secure data sharing problem in mobile cloud.

V. PROPOSED SYSTEM

Hierarchical identity based user revocation from the perceptive of encryption has been proposed. In particular, the revocation is implemented by data owners directly without any help from any third party. Compared with previous attribute-based revocation solutions, our scheme provides the following nice properties.

First, the trusted authority could be offline after system setup and key distribution, thus making it applicable in mobile cloud where the nodes in the network are unable to connect to the trusted authority after system deployment. Second, a user does not need to update the private key when user revocation occurs. Therefore, key management overhead is much lower in HIR-CP-ABE for both the users and the trusted authority. Third, the revocation mechanism enables to revoke a group of users affiliated with the same organization in a batch without influencing any other users present in cloud.

Advantages of Proposed System

- Provide affiliation-based revocation functionality for data owners.
- Secure and efficient in terms of computation, communication and storage.
- The experiments show that LDSS can greatly reduce the overhead on the client side, which only introduces a minimal additional cost on the server side.
- Such an approach is beneficial to implement a realistic data sharing security scheme on mobile devices.
- The results also show that LDSS has better performance compared to the existing ABE based access control schemes over ciphertext.
- Multiple revocation operations are merged into one, reducing the overall overhead
- In LDSS, the storage overhead needed for access control is very small compared to data files.

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. 6, Issue 5, May 2018

VI. IMPLEMENTATION & RESULT

This system is divided into five modules:

1. Data Owner Module
2. User module
3. Key Generation module.
4. Key Revocation module
5. File Access Module

MODULE DISCRIPTION

Data Owner Module

The module is used to encrypt the data with a certain access policy such that only data users whose attributes satisfy the access policy could obtain the corresponding private decryption key without any help of third party. The data provider is considered as the data owners.

User module

Data users with eligible attributes (*i.e.*, satisfying the access structure) could decrypt the ciphertext. Users whose attributes satisfy the access structure and meanwhile are not revoked by the data owners could decrypt the ciphertext. Once the correct decryption is done with the help of proper authorisation, user will get the intimation of data access.

Key Generation module.

In the key generation phase, on the one hand attributes are allocated to users as in state-of-the-art CP-ABE schemes; on the other hand a unique identity (ID) is assigned to each user. That is, both attributes and the ID are embedded into a user's private key.

Key Revocation module

In this scheme it not only supports revocation of particular users but also is capable to revoke all the users affiliated with the same organization in a batch. It also supports affiliation-based revocation.

File Access Module

The access control policy in the form of access control tree on data files to assign which attributes an authorisation should obtain if anyone wants to access a certain data file

VII. CONCLUSION AND FUTURE ENHANCEMENT

Thus in this work, the problem of how to revoke users when applying the CP-ABE scheme for secure data sharing has been investigated. Different from the previous researches on attribute based revocation, this approach focuses on identity-based revocation mechanism. The revocation mechanism remedies the deficiencies of attribute-based revocation that cannot work without the help of the trusted authority and provides more flexible and efficient

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. 6, Issue 5, May 2018

affiliation-based revocation. This System propose the primitive of HIR-CP-ABE, give its security definition and present the constructions. Through analysis and experimental evaluation, validated the security and efficiency of the proposed scheme. There are several research issues need to be further investigated. First, the revoked users' identities must be included in the ciphertext, which might lead to private information leakage. Second, in this work all the private components of a user's private key are obtained from the trusted authority. In the future will investigate how to delegate key generation to the organizations in the hierarchical identity structure tree.

REFERENCES

1. Adam Skillen and Mohammad Mannan. (2013), 'On Implementing Deniable Storage Encryption for Mobile Devices' The 20th Annual Network and Distributed System Security Symposium (NDSS).
2. Benjamin Livshits, Jaeyeon Jung (2013), 'Automatic Mediation of Privacy-Sensitive Resource Access in Smartphone Applications'. USENIX Security, pp.113-130.
3. Brakerski Z, Vaikuntanathan V. (2011), 'Efficient fully homomorphic encryption from (standard) LWE.' in: Proceeding of IEEE Symposium on Foundations of Computer Science. California, USA: IEEE press, pp. 97-106.
4. Cong Wang, Kui Ren, Shucheng Yu, and Karthik Mahendra Raje Urs (2012), 'Achieving Usable and Privacy-assured Similarity Search over Outsourced Cloud Data'. IEEE INFOCOM 2012, Orlando, Florida, March 25-30
5. Crampton J, Martin K, Wild P. (2006), 'On key assignment for hierarchical access control'. In: Computer Security Foundations Workshop. IEEE press, pp. 14-111.
6. Di Vimercati S D C, Foresti S, Jajodia S, et al. (2007), 'Over-encryption: management of access control evolution on outsourced data'. In: Proceedings of the 33rd international conference on Very large data bases. Vienna, Austria: ACM, pp. 123-134.
7. Gentry C, Halevi S (2011), 'Implementing gentry's fully-homomorphic encryption scheme. In: Advances in Cryptology'–EUROCRYPT 2011. Berlin, Heidelberg: Springer press, pp. 129-148.
8. Huang .D, X. Zhang, M. Kang, and J. Luo. Mobicloud (2010), '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.
9. Jia W, Zhu H, Cao Z, et al. SDSM (2011), 'A secure data service mechanism in mobile cloud computing'. In: Proceedings of 30th IEEE International Conference on Computer Communications. Shanghai, China: IEEE, pp. 1060-1065
10. Junzuo Lai, Robert H. Deng, Yingjiu Li ,et al (2014), 'Fully secure key-policy 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.
11. Kan Yang, Xiaohua Jia, Kui Ren: (2013), 'Attribute-based fine-grained access control with efficient revocation' in cloud storage systems. ASIACCS 2013, pp. 523-528.
12. Kan Yang, Xiaohua Jia, Kui Ren, Bo Zhang, Ruitao Xie (2013), 'DAC-MACS: Effective Data Access Control for Multiauthority Cloud Storage Systems'. IEEE Transactions on Information Forensics and Security, Vol. 8, No. 11, pp.1790-1801.
13. Kan Yang, Xiaohua Jia, Kui Ren, Ruitao Xie, Liusheng Huang (2014), 'Enabling efficient access control with dynamic policy updating for big data in the cloud'. INFOCOM 2014, pp.2013-2021.
14. Liang Xiaohui, Cao Zhenfu, Lin Huang, et al (2009), '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.
15. Maheshwari U, Vingralek R, Shapiro W (2000), '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.
16. Pirretti M, Traynor P, McDaniel P, et al (2006), 'Secure atrribute-based systems. In: Proceedings of the 13th ACM Conference on Computer and Communications Security'. New York, USA: ACM press, pp. 99-112.
17. Qihua Wang, Hongxia Jin. (2011), "Data leakage mitigation for discertionary access control in collaboration clouds". The 16th ACM Symposium on Access Control Models and Technologies (SACMAT), pp.103-122.
18. Sandhu R S, Coyne E J, Feinstein H L, et al (1996), 'Role-based access control models'. Computer, 29(2): 38-47.
19. Shi E, Bethencourt J, Chan T H H, et al (2007), 'Multi-dimensional range query over encrypted data'. in: Proceedings of Symposium on Security and Privacy (SP), IEEE press, 350-364
20. Stehlé D, Steinfeld R (2010), '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.
21. Tian X X, Wang X L, Zhou A Y. DSP RE-Encryption: (2009), 'A flexible mechanism for access control enforcement management in DaaS'. In: Proceedings of IEEE International Conference on Cloud Computing. IEEE press, pp.25-32.
22. Wang W, Li Z, Owens R, et al. (2009), 'Secure and efficient access to outsourced data'. In: Proceedings of the 2009 ACM workshop on Cloud computing security. Chicago, USA: ACM pp. 55-66.
23. Yu S., Wang C., Ren K., Lou W (2010), 'Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing'. INFOCOM 2010, pp. 534-542.
24. Yu S., Wang C., Ren K., et al. (2010), '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.