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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

LDAP Based Privacy Preserving and Multi User Audit for Cloud Computing

G.Priyanga, S.Benila

PG Scholar , Dept of C.S.E, Valliammai Engineering College,Chennai, India

Assistant Professor, Dept of C.S.E, Valliammai Engineering college, Chennai, India

ABSTRACT: Cloud computing is emerging as a prevalent data interactive paradigm to realize multiple users data remotely stored in an online cloud server. During the data accessing, different users may be in a collaborative relationship, and subsequently information sharing gets to be noteworthy to accomplish gainful advantages in the business application. The existing solutions mainly focus on the authentication to realize that a user's privative data cannot be un -authorized accessed, but neglect a subtle privacy issue during a user challenging the cloud server to request other users for data sharing. The challenged access request itself may reveal the user's privacy no matter whether or not it can obtain the data access permissions. This shared authority based directory services authentication protocol to address above privacy issue for cloud storage. Shared access authority is achieved by Lightweight Directory based authentication Protocol for create many directory services. Attribute based access control is adopted to realize that the user can only access its own data fields. AE-Attribute encryption is applied by the cloud server to store and retrieve data, and to provide data sharing among the multiple users. Meanwhile, universal compos ability model is established to prove that the SADA theoretically has the design correctness. It indicates that the proposed protocol realizing privacy-preserving data access authority sharing is attractive for multi-user collaborative cloud applications.

KEYWORDS:Cloud Computing; Cloud Server; Lightweight Directory Access Protocol; Attribute encryption; Universal Composability; Privacy Preserving

I. INTRODUCTION

Cloud computing is a promising information technology architecture for both enterprises and individuals. It launches an attractive data storage and interactive paradigm with obvious advantages, including on-demand self services, ubiquitous network access, and location independent resource pooling security and privacy issues are becoming key concerns with the increasing popularity of scheme, where an efficient and secure revocation method is proposed to solve the attribute revocation problem in the system. As described in this system, the attribute revocation method is efficient in the sense that it incurs less communication cost and computation cost, and it is secure in the sense that it can achieve both backward security (The revoked user cannot decrypt any new cipher-text that requires the revoked attribute to decrypt)and forward security (The newly joined user can also decrypt the previously published cipher-text s1, if it has sufficient attributes). Conventional security approaches mainly focus on the strong authentication to realize that a user can remotely access its own data in on-demand mode.

In this scheme does not require the server to be fully trusted, because the key update is enforced by each attribute authority not the server. Even if the server is not semi-trusted in some scenarios, this scheme can still guarantee the backward security. Then apply proposed revocable multi-authority CP-ABE scheme as the underlying techniques to construct the expressive and secure data access control scheme for multi-authority cloud storage systems.

- **Authentication:** A legal user can access its own data fields, only authorized partial or entire data fields can be identified by the legal user, and any forged or tampered data fields cannot deceive the legal user.
- **Data anonymity:** Any irrelevant entity cannot recognize the exchanged data and communication state even it intercepts the exchanged messages via an open channel.
- **User privacy**: Any irrelevant entity cannot know or guess a user's access desire, which represents a user's interest in another user's authorized data fields. If and only if the both users have mutual interests in each other's authorized data fields, the cloud server will inform the two users to realize the access permission sharing.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

- **Forward security:** Any adversary cannot correlate two communication sessions to derive the prior interrogations according to the currently captured messages.

Compared to the conference version of this work, this project has the following improvements:
Modify the framework of the scheme and market more practical to cloud storage systems, in which data owners are not involved in the key generation. Specifically, a user's secret key is not related to the owner's key, such that each user only needs to hold one secret key from each authority instead of multiple secret keys associated to multiple owners.
Improve the efficiency of the attribute revocation method. Specifically in new attribute revocation method, only the cipher-texts that associated with the revoked attribute needs to be updated, while in this system, all the cipher-text that associated with any attribute from the authority(corresponding to the revoked attribute) should be updated. Moreover, in new attribute revocation method, both the key and the cipher-text can be updated by using the same update key, instead of requiring the owner to generation update information for each cipher-text, such that owner are not required to store each random number generated during the encryption.
Highly improve the expressiveness of proposed access control scheme, where it removes the limitation that each attribute can only appear at most once in a cipher-text.

II. RELATED WORK

In [6] Aijun Ge, Jiang Zhang proposed a decentralized attribute-based encryption(ABE) system, any party can act as an authority by creating a public key and issuing private keys to different users that reflect their attributes without any collaborative computation in the setup phase of multi authority ABE schemes, thus is considered more preferable.

Disadvantages:

- A challenging open problem to construct a decentralized privacy-preserving multi authority ABE scheme in the standard model. This scheme is vulnerable to collusion attacks.

In [7] Ming Li, Shucheng Yu defines Personal health record(PHR) has emerged as a patient-centric model of health information exchange, which features storing PHRs electronically in one centralized place, such as a third-party cloud service provider. Although this greatly facilitates the management and sharing of patients personal health information(PHI),there have been serious privacy concerns about whether these service providers can be fully trusted in handling patients sensitive personal health information. To ensure patients control over their own privacy, data encryption has been proposed as a promising solution. However, key functionalities of a PHR service such as keyword searches by multiple users become especially challenging with PHRs stored in encrypted form.

Disadvantages:

The problem of authorized private searches (APS) over encrypted PHRs in cloud computing, where multiple PHR owners encrypt their health records along with a keyword index to allow searches by multiple users in the public domain.

In [2]Y. Zheng proposed Decentralized attribute-based encryption (ABE) is a variant of a multi authority ABE scheme where each authority can issue secret keys to the user independently without any cooperation and a central authority. This is in contrast to the previous constructions, where multiple authorities must be online and setup the system interactively, which is impractical. Furthermore, every authority can join or leave the system freely without the necessity of reinitializing the system.

Disadvantages:

- Different users can have access to different parts of their PHR, but the performance is degraded.
- Key-policy attribute based encryption(KP-ABE) algorithm was used; MA-ABE is not used in this paper.

III. EXISTING SYSTEM

The existing method provides security access in cloud using shared based authentication. This paper, address the above mentioned privacy issue to propose a shared authority based privacy preserving authentication protocol (SAPA) for the cloud data storage, which realizes authentication and authorization without compromising a user's private information.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

- Identify a new privacy challenge in cloud storage, and address a subtle privacy issue during a user challenging the cloud server for data sharing, in which the challenged request itself cannot reveal the user's privacy no matter whether or not it can obtain the access authority.
- Propose an authentication protocol to enhance a user's access request related privacy, and the shared access authority is achieved by anonymous access request matching mechanism.
- Apply cipher-text-policy attribute based access control to realize that a user can reliably access its own data fields, and adopt the proxy re-encryption to provide temp authorized data sharing among multiple users.

Drawbacks of Existing System

Previous System does not have the option of granting/revoking data access

- Loss of data's.
- Does not provide any privacy for private data's.
- Authentication time takes too long.

IV. PROPOSED SYSTEM

Identify a new privacy challenge in cloud storage, and address a subtle privacy issue during a user challenging the cloud server for data sharing, in which the challenged request itself cannot reveal the user's privacy no matter whether or not it can obtain the access authority.

To propose an authentication protocol to enhance a user's access request related privacy, and the shared access authority is achieved by anonymous access request matching mechanism.

Apply cipher text-policy attribute based access control to realize that a user can reliably access its own data fields, and adopt the proxy re-encryption to provide temp authorized data sharing among multiple users. Single sign on process applied to multi domain access in cloud storage.

Advantages of Proposed System

The secured system and data owner can decide whether the user can access the system or not.

V. ARCHITECTURE

Architecture diagram shows the relationship between different components of system. This diagram is very important to understand the overall concept of system. The proposed system architecture diagram shows the cloud registration using service directory, and gets access from cloud provider pool. The PHR owner provides public and private keys for accessing the PHR records by users, doctors and patients. The end user needs to view the PHR records means the permission get from any one authorized user with the identification of end use.

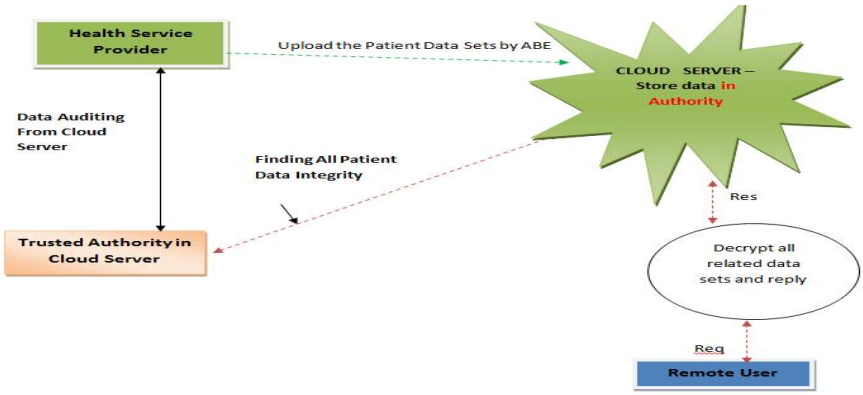

Fig.1 Architecture diagram

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

VI. MODULES

Owner Module

This module, the data owner uploads their data in the cloud server. For the security purpose the data owner encrypts the data file and then store in the cloud. The data owner can change the policy over data files by updating the expiration time. The Data owner can have capable of manipulating the encrypted data file. And the data owner can set the access privilege to the encrypted data file. The main goal of it framework is to provide secure patient-centric BR access and efficient key management at the same time. The key idea is to divide the system into multiple security domains (namely, *public domains* (PUDs) and *personal domains* (PSDs)) according to the different users' data access requirements. The PUDs consist of users who make access based on their professional roles, such as doctors, nurses and medical researchers. In practice, a PUD can be mapped to an independent sector in the society, such as the health care, government or insurance sector. For each PSD, its users are personally associated with a data owner (such as family members or close friends), and they make accesses to BRs based on access rights assigned by the owner.
Each data owner (e.g., patient) is a trusted authority of her own PSD, who uses a KP-ABE system to manage the secret keys and access rights of users in her PSD. Since the users are personally known by the BR owner, to realize patient-centric access, the owner is at the best position to grant user access privileges on a case-by-case basis. For PSD, *data attributes* are defined which refer to the intrinsic properties of the BR data, such as the category of a BR file. For the purpose of PSD access, each BR file is labeled with its data attributes, while the key size is only linear with the number of file categories a user can access. Since the number of users in a PSD is often small, it reduces the burden for the owner. When encrypting the data for PSD, all that the owner needs to know is the intrinsic data properties**.**

Cloud Server Module

The cloud service provider manages a cloud to provide data storage service. Data owners encrypt their data files and store them in the cloud for sharing with data consumers. To access the shared data files, data consumers download encrypted data files of their interest from the cloud and then decrypt them. In this paper consider the server to be semi-trusted, i.e., honest but curious as those in and . That means the server will try to find out as much secret information in the stored BR files as possible, but they will honestly follow the protocol in general. On the other hand, some users will also try to access the files beyond their privileges. For example, a pharmacy may want to obtain the prescriptions of patients for marketing and boosting its profits. To do so, they may collude with other users, or even with the server. In addition, Let assume each party in the system is preloaded with a public/private key pair, and entity authentication can be done by traditional challenge-response protocols.

Attribute Based Access Policy Module

The owners upload ABE-encrypted BR files to the server. Each owner's BR file is encrypted both under a certain fine grained and role-based access policy for users from the PUD to access, and under a selected set of data attributes that allows access from users in the PSD. Only authorized users can decrypt the BR files, excluding the server. In this framework, there are multiple SDs, multiple owners, multiple AAs, and multiple users. In addition, two ABE systems are involved. Then term the users having read and write access as data readers and contributors, respectively.

Cipher text-Policy Attribute-base Encryption (CP-ABE) is regarded as one of the most suitable technologies for data access control in cloud storage. In almost all existing CP-ABE schemes, it is assumed that there is only one authority in the system responsible for issuing attributes to the users. However, in many applications, there are multiple authorities co-exist in a system and each authority is able to issue attributes independently. In this paper design an access control framework for multi-authority systems and propose an efficient and secure multi-authority access control scheme for cloud storage. First design an efficient multi-authority CP-ABE scheme that does not require a global authority and can support any LSSS access structure .Then proved its security in the random oracle model. It also propose a new technique to solve the attribute revocation problem in multi-authority CP-ABE systems. The analysis and simulation results show that the multi-authority access control scheme is scalable and efficient.

Data Consumer Module

This module, user status is revoked to earlier state, when t is disabled by human error or miss used by others. User revocation is processed in two stages. In first step, disabled/ noted user will get message about its authentication fail on

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

allowed trines. User has to verify their identity to prove the uniqueness. Once the identity is confirmed new access code or secret key will be send by data owner from the server.

All the legal users in the system can freely query any interested encrypted and decrypted data. Upon receiving the data from the server, the user runs the decryption algorithm to decrypt the cipher text by using its secret keys from different AAs. Only attributes the user possesses satisfy the access structure defined in the cipher text CT, the user can get the content key.

VII. CONCLUSION AND FUTURE WORK

This paper improving the Security on Public Health Record System in Cloud Computing. And also made a detailed study about what are the techniques is needed for security the Health Record System. Attribute Based Encryption is the good technique to securing the Health records. It is efficient in the Conjunctive Property. But somewhat limitations on MA-ABE in real time with the property of Disjunctive as well as it had the little bit problem while revocation. Because it can be affect the non-revoked users. So move to the Attribute Based Broadcast Encryption. It satisfies the Disjunctive Property also and handles the revocation perfectly. Identity Based Encryption is the better way to provide the authentication for the Public Health Record System. Homomorphism encryption with data auditing is used to verify the trustworthiness of third party auditor.

REFERENCES

1. Sahai and B. Waters. "Fuzzy Identity Based Encryption.", In Advances in Cryptology – Euro-crypt, volume 3494 of LNCS, pages 457–473. Springer, 2005.
2. Yao Zheng "Privacy-Preserving Personal Health Record System Using Attribute-Based Encryption".
3. Li, M., Lou ,W., Ren , K., " Data security and privacy in wireless body area networks", IEEE Wireless Communications Magazine (February 2010).
4. M.Li, S. Yu, K. Ren, and W. Lou, "Securing Personal Health Records in Cloud Computing: Patient -Centric and Fine-Grained Data Access Control in Multi-Owner Settings", Proc. Sixth Int l ICST Conf. Security and Privacy in Comm. Networks (SecureComm 10), pp. 89 -106, Sept. 2010.
5. Prof.Y.B.Gurav *et al*, International Journal of Computer Science and Mobile Computing, Vol.3 Issue.2, February- 2014, pg. 617-625 © ***2014, IJCSMC All Rights Reserved 625***
6. V.Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data,"Proc. 13th ACM Conf. Computer and Comm. Security (CCS ″06),pp. 89-98, 2006.
7. Aijun Ge, Jiang Zhang, Rui Zhang, Chuangui Ma, and Zhenfeng Zhang"Security Analysis of a Privacy-Preserving Decentralized Key-Policy Attribute-Based Encryption Scheme" IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 24, NO. 11, NOVEMBER 2013
8. Ming Li_, Shucheng Yuy, Ning Cao_ and Wenjing Lou "Authorized Private Keyword Search over Encrypted Personal Health Records in Cloud Computing".