ISSN: 0974-2115
www.jchps.com Journal of Chemical and Pharmaceutical Sciences

Optimal Identity Preserving Mechanism Using Attribute Based Encryption in Cloud Environment

Gladwin A
Department of Information Technology, Jeppiaar Engineering College
***Correspondingauthor:E-Mail:meetgladwin@gmail.com**

ABSTRACT

The increasing use of smart phones gives on the go computational capability and provides enormous data storage. Due to limited data storage and battery life it is impossible for smart phones to provide all kinds of service and data storage. Cloud networks offer optimal data backup and online services which reduce the computation and data storage overhead. For secure data sharing and storage user share their personal information for authentication and authorization. Sharing personal data in a public cloud lead to lots of security problems. I propose a novel method to protect sharing of personal data in a secure manner. It includes hiding the identity of user information as well as provide high level authentication. It also provides efficient user revocation in case if user shares data across a group of users.

KEY WORDS: Attribute-based encryption, homomorphic encryption, Identity Preserving.

I. INTRODUCTION

Cloud computing is an emerging trend in mostly all kinds of industry. Based upon virtualization and distributed nature of cloud computing leads to reduced cost and operational efficiency and flexibility. Cloud computing reduce the hardware and software cost since it can provide scalable and on the go operational features from where ever and whenever you want the resources. Even though cloud computing provides efficient mobile computing and hardware sharing; security problem is a major concern in cloud. One of the important security breaches is the data secrecy. Data owners outsource their confidential data to various remote cloud servers for storage and manipulation. Those data can be accessed through the Cloud Solution Provider (CSP) resource centre. Even though CSP provides security solutions to the cloud operations there occurs various security problems since it can be compromised by any third available in the network.

For protecting user data and to provide access privileges data owners may need to share their personal and profile information with CSP. Hence if CSP can be attacked it leads to leakage of data owner's private information. Thus it is very important to preserve the data owner's confidential data and user privacy. A feasible solution is to encrypt the outsourcing data. Using this method only authorized user can only decrypt the data with the corresponding decryption key. Even CSP and intruders cannot able to decrypt the encrypted data. Therefore, data encryption is a better method to satisfy the security requirements in cloud computing. Even though protecting privacy information is major security concern.

Digital rights management (DRM) is one of the popular method in protecting copyrighted content based on providing dynamic licensing, giving privileged access control mechanism and content based encryption scheme. **Related work:** In this section, we discuss the relevant work about DRM in cloud computing.

A typical approach for protecting data confidentiality is to encrypt the data with an encryption key before storing it to cloud database. Han, introduced an identity-based PRE data storage scheme which is applicable to cloud computing as it can able to hold both intra-domain and inter-domain concern. In this scheme, the access key can be manipulated by the data provider independently without the help of the key server.

Access control is a major concern in security mechanism which provides limited access in a controlled manner. Attribute Based Encryption ABE provides efficient access control mechanism. The notion ABE was introduced by Sahai and Waters for fuzzy identity-based encryption. In ABE both the encrypted message and data owner's decryption keys are matched with a set of attributes. Data owners can decrypt the original data only if there is match between decryption key and cipher text.

Data aggregation is a kind of data gathering process in which data is formatted in summarized manner. Cloud computing provides on the go demand based storage service for data to data owners anywhere and anytime. It stores the data in a common centralized data server present somewhere in a remote location. Corena purposed architecture based on additive homomorphic encryption and secret distribution schemes to save data securely while still granting fast gathering queries at an outsourced unreliable cloud server.

Privacy preserving is one of the major security concerns in cloud computing. Most of the research areas try to preserve data from external hackers in the cloud. Only few of the works try to work towards preserving the user identity through a cloud network. Perlman, introduced a privacy-preserving DRM solution that grants users to asset content anonymously from a data owner and access the data without being trailed.

Proposed Scheme:

Design goals: The design goals of the proposed scheme are summarized as follows:

- Key and data confidentiality. Pirated users who do not bear ample attributes gratifying the access policy should be interrupted from decrypting the key and data.

- Fine-grained access control. The data providers can gratify vivid access method for data, and the access policy should be expandable.
- Efficient revocation. Rather than regularly re-encrypting data and recreating new secret keys, the key server can take leverage of the generous resource data in the cloud to abolish attributes and illicit users readily and immediately.
- Privacy-preserving dynamic usage control. The conventional authority encrypted by the user's public key are saved in the cloud database, which grant the users to utilize the data anytime anywhere. The license server in the cloud can be able to amend the users' conventional authority actively without revealing the users' privacy.
- Scalability and efficiency. Since the number of users may be unpredictable and unaccountable, the proposed scheme should be highly scalable and efficient.

System model: The main objective of our architecture is to equip a secure data sharing.

The main scheme is to partition the Cloud Encryption Key CEK into two sectors: Content Master Key CMK and Assistant Key AK. Both the keys are preserved in a secure manner and distributed among the users independently. As shown in Fig.1, the system model of the proposed strategy contains the following entities:

- Cloud storage. The cloud storage is an entity which affords a data storage service and on the go data processing service anywhere and anytime.
- Cloud service provider provides data outsourcing and data subscription service. Encrypted data from the data owners are deployed out to cloud database through the Cloud Service Provider, and the Cloud Service Provider is also in control of data agreement from the users and certificate sharing to the users.

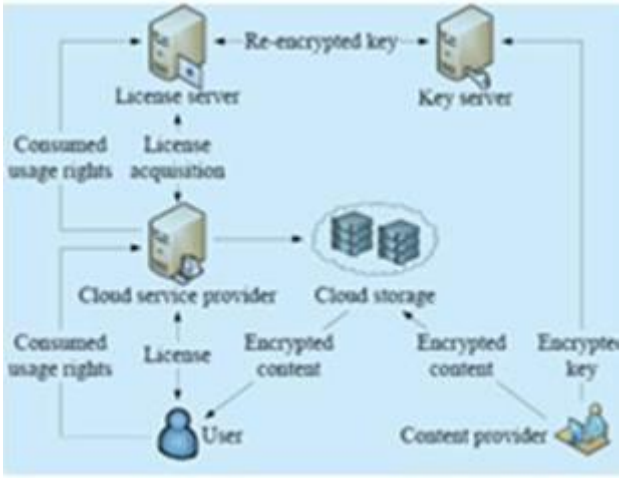

Figure.1. System model

- License server. The license server develops and supplies the certificates for the users when receiving the certificate procurement from the Cloud Service Provider. The certificate consists of the encrypted *Assistant Key AK*. It also refuses to give away usage access claim to the user if the user's attributes did not compromise the AP or the user is reverted.
- Key server. The key server provides the public and secret keys for the networking cloud system. It provides various attributes to different users in the cloud, and provides attribute secret keys to the cloud users.

It also re-encrypts the *Assistant Key AK* for cloud users when they pick up the license.

- Content provider wishes to outsource their data to cloud storage provided by the Cloud Service Provider, for the need of using cheap and low energy consuming storage assets. The content providers encrypt their data before storing them in an external database. The principal part of the ciphertext includes the *Content Master Key* encrypted with the access rights.
- The user wants to access the data which is stored in a remote cloud database. If a user having a set of corresponding attributes compromising the *Authentication Protocol* of the CT, he will be given access rights to decrypt and download the data from the cloud server.

2. METHODS

Content encryption: The source message sender evaluate Encrypt algorithm to encrypt the message data The source message sender initially produces the *CEK* with arbitrary *CMK* and arbitrary *AK*, and then encrypts the message data *M* with *CEK*, generates the value *C* as follows:

$$CEK = CMK + AK$$

$$C = Enc(CEK, M)$$

The source message sender then inputs the value *PK* and AP to encrypt the *CMK*, produces the result *CMKA* as follows: $CMK = CMK \cdot e'(q, tn_{AP_1})$

Where *t* is a arbitrary item in Zp, and *N* is the count of unified conjuctive clauses *CC* in *AP*, *ni* is the count of attributes in the *i*th unified conjunctive section *CCi*, and *nA* is the LCM of *n1*,…,*nN*.

The source message sender produces the ciphertext and send out the *CT* to the CSP

Key update: On obtaining the user's certificate purchase offer, the key server evaluates *ReEncrypt* method to re-encrypt the *AKCP* with *RK*, and generates the result *AKU*:

$$AK_u = e' (AK_{cp}, RK)$$

Content decryption: The receiver uses SK_U to regain *AK* as follows:

$$AK = AK_0 / AK_U^{1/SKU}$$

If the user's *UR* are effective, the user uses the *CMK* and *AK* to generate the *CEK*, and service the *CEK* to break the *CT* as follows:

$CEK = CMK + AK$

$M = Dec(CEK,C)$

3. RESULTS AND DISCUSSION

Security analysis: The proposed scheme grants access of data only to licensed users. The user can decrypt the message if and only if it has an identical pair of attributes and active control license. Hence this method permits rights of message only to licensed users. The proposed scheme assures confidentiality of the message across illegal users and the inquisitive CSP and license grant server in the cloud.

Performance analysis: If a user is described by *n* attributes, the key generation server evaluate *O*(*n*) point product to produce the *ASK*. Let the length of user's key is *m* and the count of unified conjunctive section in *AP* is *N*, the message sender requires to encrypt the message using the *CEK*, and evaluate *O*(*N*) number of exponentiation operations to the result the encrypted *CMK*, and evaluate *O*(*m*) number of exponentiation operations to output the encrypted *AK*.

To decrypt the *CT*, the user whose attributes justify the access control policy and whose control access rights are major requirement to evaluate 2O(1) bilinear map methods to restore the *CMK* and *AK*. Let the length of usage access rights is *s*, the license grant server requires to implement only one modular summation in mean for the effective access control, thus the computation complexity is *O*(*s*) bit operations. The entire computation complexity of the pattern is shown in Table 1

Table.1.Computation complexity of proposed scheme

Properties	Complexity
Message encryption	O(N) + O(m)
Message decryption	2O(1)
Active usage control	O(r)
Attribute revocation	O(1)
User revocation	O(1)

4. CONCLUSION

In this paper, we propose an optimal Digital Rights Management DRM strategy with secure key management and efficient access control in the cloud environment. The proposed model consists of a secure data sharing mechanism which not only protects user's data but also their confidential private information from external threats. Thereby it provides data security as well as Privacy preserving. The system model uses two sectors of Cloud Encryption Key which includes Content Master Key CMK and Assistant Key AK. Both provides license to the users based upon the attributes of the users which is hidden from the intermediate cloud decrypting mechanisms.

REFERENCES

Cheng Hongbing, Rong Chunming, Tan Zhenghua, Identity based encryption and biometric authentication scheme for secure data access in cloud computing, Chinese Journal of Electronics, 21(2), 2012, 254-259.

Cheng Yong, Wang Zhiying, MA Jun, Efficient revocation in ciphertext-policy attribute- based encryption based cryptographic cloud storage, Journal of Zhejiang University, Science C, 14(2), 2013, 85-97.

Ma Zhaofeng, Fan Kefeng, Chen Ming, Trusted digital rights management protocol supporting for time and space constraint, Journal on Communications, 29(10), 2008, 153-164.

Petrlic R, Proxy re-encryption in a privacy-preserving cloud computing DRM scheme, Proceedings of 4th International Symposium, Melbourne, Australia, 2012, 194-211.

Petrlic R, Sorge C, Privacy-preserving DRM for cloud computing, Proceedings of 26th IEEE International Conference on Advanced Information Networking and Applications Workshops, Fukuoka, Japan, 2012, 1286-1291.

Tran D.H, Nguyen H.L, Wei Zhao, Towards security in sharing data on cloud-based social networks, Proceedings of 8th International Conference on Information, Communications and Signal Processing, December, 2011, 13- 16.

Wan Zhiguo, Liu June, Deng RH, A hierarchical attribute-based solution for flexible and scalable access control in cloud computing, IEEE Transactions on Information Forensics and Security, 7(2), 2012, 743-754.

Wang Guojun, Liu Qun, Wu Jie, Hierarchical attribute-based encryption and scalable user revocation for sharing data in cloud servers, Computers and Security, 30(5), 2011, 320-331.

Wang Qian, Wang Cong, Ren Kui, Enabling public auditability and data dynamics for storage security in cloud computing, IEEE Transactions on Parallel and Distributed Systems, 22(5), 2011, 847-859.

Zhang Zhiyong, PEI Qingqi, MA Jianfeng, Establishing multi-party trust architecture for DRM by using game-theoretic analysis of security policies, Chinese Journal of Electronics, 18(3), 2009, 519-524.