International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 – 5161

Available at http://inpressco.com/category/ijcet

Research Article

Efficient Fine-grained access control for Shared Data using Proxy Re-encryption

Sangita B. Chavan†* and Ashish Kumar†

†G.H. Raisoni COE, Ahmednagar, Savitribai Phule Pune University

Accepted 30 July 2016, Available online 02 Aug 2016, **Vol.6, No.4 (Aug 2016)**

Abstract

Cloud is quickly developing in today's business sector. It turns out to be to a great extent helpless to utilize cloud administrations to share information in a companion circle in the distributed computing environment. Due quick improvement of flexible cloud administrations, it is not possible to execute full lifecycle protection security, access control turns into a troublesome undertaking, particularly when offer touchy information on cloud servers. Additionally to share reason we require effective strategy and secure system over cloud. The current KP-TSABE is concentrating on information security over particular day and age rather than full lifecycle protection arrangement. In this paper we proposed new intermediary proxy re-encryption technique. We foresee that quick and secure re-encryption will turn out to be progressively famous as a technique for overseeing scrambled document frameworks we display new re-encryption conspires that understand a more grounded thought of security, and for adding access control to a protected record system. Performance estimations of our trial document framework exhibit that intermediary re-encryption can work successfully by and by.

Keywords: *Proxy re-encryption, Cloud Computing, privacy-preserving, fine-grained access control, full lifecycle.*

Introduction

Cloud computing has wide range of scope these days. Cloud provides large amount of virtual environment hiding the platform and operating systems to the user. User gets to use the resources. User has to pay as per the use of the resources of the cloud. Now cloud service providers are offering cloud services instead of buying a software. Large amount of data gets uploaded on the cloud and shared by millions of the users. User need not to purchase the resources. As the data gets uploaded by the user every day it is critical task to manage Ease of Use as well as to provide security to data on the cloud.

When we are using the word Moving to Cloud, means we have shifted existing services or data to cloud computing but whenever moving information to cloud information can be very sensitive (Organization business profile, financial information, client records, personal information) and those shared data on a cloud storage has a risk of information leakage caused by service provider's abuse. Sometimes need to migrated data from one cloud to other cloud for outsourcing and share it for cloud searching, so that cloud is complex and hence security measures are not simple too. It mostly becomes very tedious task for security in big data environment and information in cross cloud .In order to protect data, the data owner encrypts data shared on the cloud storage so that only authorized users can decrypt. Sharing sensitive information on cloud, requires huge amount of security. There are no of techniques available for providing security to shared data but each method has some limitations to achieve the highest amount of security (Jinbo Xiong *et al*, 2014) One of the solutions for providing authenticity to sensitive data is self-expiration time and fine-grained access control. The sensitive and shared information should be able to destruct itself after expiration time provided by user and also providing proxy re-encryption technique for providing full lifecycle privacy to the sensitive information. KP-TSABE (Jinbo Xiong *et al*, 2014). is achieving secure self-destructing scheme for data sharing in cloud computing and efficient privacy of shared data between authentic users and organizations. In such a system, decryption of cipher text is possible only if set of attributes of user key matches the set of attribute set and set of time intervals.

Literature Survey

There are many techniques available for protecting information in cloud and each technique has its own advantages and disadvantages. Cloud computing has been providing various and versatile services for

*Corresponding author: **Sangita B. Chavan** is a ME Scholar; **Ashish Kumar** is working as Assistant Professor

sharing information over the internet for electronic business as well for personal use from anywhere and anytime. The main task is providing protection to shared data.

P. Tysowski *et al*. Designed an attribute based proxy re- encryption system (P. Tysowski *et al* 2013) In this scheme a delegator assigns the proxy to transform a cipher. This cipher text can be decrypted using attribute keys into another cipher text that a specific person can decrypt. The holding attributes that are used to decrypt the cipher text are different between the delegator and the delegate. The proxy cannot obtain the content of cipher text nor do the private attribute keys of the delegator while the re-encryption procedure. In addition to this the cipher text can be successfully re-encrypted a number of times if the delegator decrypts the cipher text. Thus the attribute based proxy re-encryption protocol has a very rich access policy and dynamic membership.

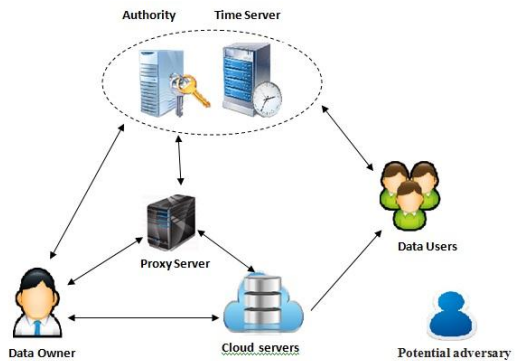
In the Full PP scheme (J. Xiong *et al*, 2014) the sensitive data is first encrypted into the cipher text, which is broken into extracted cipher text and encapsulated cipher text using an extracting algorithmic procedure. Full PP is able to provide entire life cycle privacy protection for sensitive data of the users by making it unreadable before a predefined time and is automatically destroyed after expiration. An ideal feature of the FullPP scheme is it does not make use of the assumption that No attacks on SDO before it expires. The ID-TRE is introduced and transformation algorithm to make the FullPP scheme obey the security requirements and also resist three types of possible attacks. The performance result measurement shows that the proposed FullPP scheme is very efficient than the ones that already exist.

Implementation Detail

The proposed System is secure self-destructing scheme for data sharing in cloud computing for achieving powerful and efficient privacy of shared data between authentic users and organizations.

1. *System Architecture*

Specifically, The Proposed system model by dividing the KP-TSABE using proxy re-encryption scheme into the following seven entities as shown in Fig 1.



Data Owner request public key from authority. It gets key from authority then it request time from timeserver and it gets time from timeserver. It gives access tree with some logical expression and upload file in encrypted format. Data user who wants to access the document must satisfy the owner given access tree and time, user takes private key from authority and time from time server. If the attributes of user and user time matches with owner then it is eligible to access document. Potential adversary is polynomial time adversary, it declares the attribute set and it generates repeated private keys corresponding too many access structures.

2. *Algorithms*

Proposed scheme is composed of seven algorithms: Setup, Encrypt, KeyGenerate, ReKey-Generate, ReEncrypt, ReKey, Decrypt (L. Cheung *et al*,2007; J. Bethencourt *et al*,2007)

- **Setup (1^{λ} ,U):** This algorithm is run by the Authority and takes as input the security parameter 1^{λ} and universe description of attributes U then generates the system master key MSK and public parameters PK. ver is initialized as 1.
- **Encrypt(M,AS,PK,T_s):** This algorithm takes as input a message M, an access structure AS, and current public parameters PK and the set of time intervals T_s in which every element in T_s is associated with a corresponding attribute in AS and outputs a cipher text CT.
- **KeyGenerate(MSK,ϒ,T'):** It takes as input current system master key MSK ,the access tree ϒ and the time set T'. Every attribute x in ϒ is associated with a time instant $t_c \in T'$. It outputs a user secret key SK_1 which contains ϒ.
- **ReKeyGenerate(MSK,Ÿ,T'):** This algorithm takes as input an attribute set that includes attributes for update, and current master key MSK and the time set T'. It outputs the new master key MSK', the new public key PK' (computation of PK' can be delegated to proxy servers), and a set of proxy re-keys rk for all the attributes in the attribute universe U. ver is increased by 1.
- **ReEncrypt(CT, rk,θ,T_s):**It takes as input a cipher text CT, the set of proxy re-keys rk having the same version with CT, the set of time intervals T_s and a set of attributes θ which includes all the attributes in CTs access structure with proxy re-key not being 1 in rk. It outputs a re-encrypted cipher text CT' with the same access structure as CT.
- **ReKey($\bar{D}$, rk , β, T'):** It takes as input the component $\bar{D}$ of a user secret key SK_1, the set of proxy re-keys rk having the same version with SK_1, the time set T'and a set of attributes β which includes all the attributes in SK_1 with proxy re-key not being 1 in rk. It outputs updated user secret key SK_2 components $\bar{D}'$.

- **Decrypt(CT, PK, SK_1,SK_2):** It takes as input a cipher text CT, public parameters PK, the user secret key SK_1 and updated user secret key SK_2 having the same version with CT. It outputs the message M if the attribute set of SK_1 ,SK_2 satisfies the cipher text access structure.

3. Module Description

a. User Registration

Data owner and data user have to register. Then owner or user login using that registered id and password user. then owner upload document to cloud in encrypted format using public parameter, attribute set and set of time interval. Data owner takes the public parameter from authority. It takes time interval from time server. Owner gives access tree using public param and time interval. It upload file to cloud server.

b. Encryption of Data

Encryption module is the security module. In the system which undertakes the work of encrypting uploaded data and decrypting the downloaded data. Data being store on public cloud, so needs to be encrypted. The Data is encrypted using RSA or BLS Algorithm as both being efficient and simple to implement but difficult to break.

c. Fine-grained access control during the authorization period

The register data user which wants to access the document takes decryption key from authority. It takes time from time server. If access tree and time given by owner matches the user time and attribute, then only user is able to access the document.

Conclusion

The electronic business is rapidly growing and cloud computing is modern step for electronic business for providing on demand service with pay as per use facilities. The shared data contains the sensitive information and need to provide full lifecycle privacy to sensitive data.

There are so many schemes available but each one have own merits and demerits. KP-STABE provides the highest amount of security and fine-grained access control. Also re-encryption adds security level for shared data in cloud computing.

Acknowledgment

I would like to sincere thanks to the peoples who support and help specially my guide **Ashish Kumar** for his great help from beginning to end.

References

Jinbo Xiong, Ximeng Liu, Zhiqiang Yao, Jianfeng Ma, Qi Li, Kui Geng, and Patrick S. Chen (2014), A Secure Data Self-Destructing Scheme in Cloud Computing, IEEE Transaction on Cloud computing, 2(4) pp. 448-458.

B. Wang, B. Li, and H. Li, (2014), Oruta: Privacy-preserving public auditing for shared data in the cloud, IEEE Transactions on Cloud Computing , 2(1), pp 43-56.

J. Xiong, Z. Yao, J. Ma, X. Liu, Q. Li, and J. Ma (2014) Priam: Privacy preserving identity and access management scheme in cloud, KSII Trans. Internet Inf. Syst., 08(01), pp 282-304.

J. Xiong, F. Li, J. Ma, X. Liu, Z. Yao, and P. S. Chen, (2014), A full lifecycle privacy protection scheme for sensitive data in cloud computing, Peer-to-peer network Appl.

P. Jamshidi, A. Ahmad, and C. Pahl (2013), Cloud migration research: A systematic review, IEEE Trans. Cloud Comput. 01(02), pp 142-157.

P. Tysowski and M. Hasan (Jul. 2013), Hybrid attribute- and re-encryption based key management for secure and scalable mobile applications in clouds, IEEE Trans. Cloud Comput., vol. 1, no. 2, pp. 172–186

J. Xiong, F. Li, J. Ma, X. Liu, Z. Yao, and P. S. Chen (Jun. 2014), A full lifecycle privacy protection scheme for sensitive data in cloud computing, Peer-to-Peer Netw. Appl., DOI:10.1007/s12083-014-0295-x.

X. Liang, Z. Cao, H. Lin, J. Shao (2009,), Attribute based proxy re-encryption with delegating capabilities, in: Proceedings of the 4th International Symposium on Information, Computer, and Communications Security, ASIACCS'09, ACM,276-286.

L. Cheung and C. Newport (2007) Provably Secure Ciphertext Policy ABE. In Proc. of CCS'07, New York, NY, USA.

J. Bethencourt, A. Sahai, and B. Waters (2007) Ciphertext-Policy Attribute-Based Encryption. In Proc. of SP'07, Washington, DC, USA.