ABHIYANTRIKI
An International Journal of Engineering & Technology
(A Peer Reviewed & Indexed Journal)
Vol. 3, No. 5 (May, 2016) http://www.aijet.in/ eISSN: 2394-627X

An Approach for Privacy Preserving and Multi-Sharing Control using Proxy Re-encryption in Big Data Storage Services

G. T. Raju
Head
Deptt. of Computer Science & Engineering
RNS Institute of Technology, Bengaluru, India

Skanditha Satish*
PG Student
Deptt. of Computer Science & Engineering
RNS Institute of Technology, Bengaluru, India

Abstract

In recent years, the need for security in big data storage services has been a major bottleneck for the users of big data. The basic prerequisite is to ensure the confidentiality of the data and the anonymity of the service clients simultaneously, which have been the vital aspects of privacy. In addition, the service should also provide a method where fine-grained encrypted data, in the form of cipher text, to be shared by the data owner among the various data users under some specific conditions. Hence, a privacy preserving cipher text multi-sharing mechanism is proposed to achieve the above properties. This mechanism combines the advantages of proxy re-encryption along with the anonymous techniques to securely and conditionally share the cipher text multiple times without divulging both the knowledge of the underlying message and the identity of the cipher text senders and recipients.

Keywords*: Privacy preserving, Anonymity, Cipher-text, Multi-sharing control, Proxy re-encryption.*

****Author for correspondence*** skandithasatish@gmail.com

1. Introduction

Big Data is defined as a large amount of data that is used in the traditional data processing applications. The term “Big Data” often refers to the use of predictive analysis or some advanced methodologies to extract value from data or large amounts of data sets. Sources of these data sets are increasing rapidly day-by-day as they are derived from information-sensing mobile devices, remote sensors, microphones and other wireless sensor networks. Accuracy in big data may often require confident decision making strategies which can result in greater operational efficiency, cost reduction and reduced risk. Big data usually contains data sets whose size are very large beyond the potential of commonly used software tools to capture, manage and process data within a predefined elapsed time. Data sets may be of the size of few dozen terabytes to many petabytes of data. Security and Privacy issues are the most important concern for the basic functionality of Big Data. An important security requirement of the big data storage service is to ensure the security and privacy of the data. But many existing mechanisms are in practice to

satisfy this requirement. For example, considering the Public Key Encryption (PKE) permits the sender to encrypt the data under the public key of the receiver such that nobody except the substantial receiver can secure access to the data. In any case this does not fulfill all the requirements of data clients or users in the context of big data storage service. The existing privacy preserving mechanisms used in big data storage services fails to provide the confidentiality of the data and the anonymity of the service clients. The problem here is to provide a secure, privacy preserving cipher-text multi sharing mechanism by combining the merits of proxy re-encryption [1].

To overcome the above drawbacks, we proposed a privacy preserving multi-sharing control mechanism. It allows a semi-trusted party, called proxy, to transform a cipher-text intended for a user into a cipher-text of the same message intended for another user without leaking knowledge of either the decryption keys or the message. The workload of data owner is now transferred to the proxy, and the "on-line all the time" requirement is unnecessary. The proposed system also achieves the properties of Anonymity, Multi-Sharing Control, Multiple updates by the receiver by a employing a Proxy Re-Encryption (PRE) method in the context of Identity-Based (IBE) setting. This work concentrates on the identity-based cryptographic setting. To employ PRE in the IBE setting, a notion called as Identity-Based Proxy Re-Encryption (IBPRE) is defined, which offers a practical solution for access control in networked file storage and secure email with IBE. To capture privacy-preserving property and cipher-text's recipient update simultaneously, an anonymous IBPRE system, which is CCA security model, is proposed.

2. Related Work

Need for Privacy in Big Data: Big Data provides a large number of chances for enterprise in industries. Hence, security or privacy is a treat in big data, and then it results in serious legal problems and damage to the stature of the enterprise in industries. As the big data technology increases, information classification has become crucial, since various industries use different methodologies to store and analyze very large sets of data. Due to the extensive use of big data in business, many industries are still tackling with the data privacy issues. So to make big data storage services more secure and privacy preserving, many techniques such as encryption, decryption, fraud detection and logging have been introduced.

Proxy Re-Encryption: In 1998, Blaze, Bluemer and Strauss [2] proposed the concept of "Atomic proxy Re-Encryption" in which a semi-trusted party, called as Proxy, computes a function which converts the cipher-text for the receiver into the cipher-text for the sender without revealing underlying plain text and knowledge of either the decryption keys or the message. But this scheme has an inherent limitation: it is bidirectional. Hence this scheme is useful only when there is a fully trusted relationship between the intended sender and the receiver. This concept has many other drawbacks: The delegation process in this scheme is transitive. This means that the proxy can create delegation rights between the two parties which have never agreed upon the delegation process. Another major drawback of this scheme is that if the proxy collides with the intended receiver, then the proxy can recover the receivers' secret key. To overcome the above drawbacks Ivan and Dodis [3] proposed a unidirectional proxy re-encryption and IBE (Identity Bases-Encryption) scheme in which the user's secret key is shared between the two parties. This scheme also solved the problem of proxy assigning the delegation rights. In this scheme the secret key of sender is divided in two parts and each part is distributed to the proxy and the

receiver respectively. Hence, this scheme is more advantageous than the other schemes. But this scheme also has many drawbacks. These schemes do not change the cipher-text for the sender into the cipher-text for the receiver in the purest and easiest form. This scheme also requires the receiver to store additional secret keys to delegate the decryption process. This causes a major problem when the proxy and any delegate collide as both of them can decrypt everyone else's message.

Anonymous IB-PRE: The anonymous IB-PRE scheme [4] allows proxy to translate the encryption using the identity of the intended receiver to be computed into the identity of the intended sender. The proxy uses proxy keys to perform this translation without the knowledge of plaintext as well as the sender and receiver. The Identity-Based Encryption scheme requests these proxy keys from a fully trusted party called as the Private Key Generator (PKG). But in practice these keys can be generated by the PKG directly. From a theoretical view, PKG generating the proxy keys makes the problem of finding IB-PRE schemes quite unchallenging. Considering the practical view, it is highly undesirable to use PKG for the generation of proxy keys as it would cause a considerable bottleneck in many applications. The properties of IB-PRE are as follows:

- Uni-directionality: A unidirectional scheme permits user A to delegate to user B, without permitting user A to decrypt user B's cipher-texts.
- Non-Interactivity: Non-interactive schemes permit user A to construct a proxy key without the participation of B or the Private Key Generator
- Multi-use: A multi-use scheme permits the proxy to perform multiple re-encryptions on a single cipher-text.
- Non-transitivity: In a non-transitive scheme, the proxy is not authorized to re-delegate decryption rights.

3. Proposed Work

Consider a real-time scenario. A hospital stores its patients' medical records in a cloud storage system and all these records encrypted to avoid the cloud server from accessing to any patient's medical data. After a record is encrypted and uploaded to the cloud, only those specified doctors who are diagnosing the patient can gain access to the record. By using some traditional PKE or Identity-Based Encryption (IBE), the confidentiality of the record can be protected effectively. But we cannot prevent some sensitive personal information from being leaked to the cloud server but also the public completely. This is because PKE or IBE do not consider the anonymity of both the cipher-text sender and receiver. Also anyone with capability of obtaining a cipher-text, may know whose public key the cipher-text is encrypted under, who is usually the owner of the cipher-text, such that the patient associated with the cipher-text can be easily identified. Similarly, the recipient of the cipher-text, e.g., Neurology department can be known from the cipher-text without any difficulty as well. This has a serious effect on the privacy of patient. Additionally, a patient might be transferred to more than one medical department in different phases of treatment. The corresponding medical records have to be then to be converted to the cipher-text of the corresponding receivers so that it can be shared among the departments. Therefore, the update of cipher-text recipient is mandatory. In short, a fine-grained cipher-text update for receivers is necessary for the cipher-text to be shared conditionally with others. The patient has rights to decide who can gain access to the record, and which kinds of data are allowed for access. This fine-grained control prevents a data sharing mechanism from being limited to the "all-or-nothing" share mode which means that the data can be shared with

everyone or with no-one depending upon the access given by data owner. This proposed scheme aims to solve the above problems. To preserve anonymity, a well-known encryption mechanisms, called as anonymous IBE is proposed, which aims to provide anonymity to the source and the destination data. But the methods in the above anonymous IBE scheme cannot support the update of cipher-text receiver. There are many novel ways to update cipher-text's recipient. One of the most commonly used methods is the decrypt-then-re-encrypt mode which is employed by the data owner. If the encrypted data is either a group of data or a network log, the decryption and re-encryption using this method can be time consumed and computation-effective. This method also requires the data owner to be available at all times. Hence, a fully trusted third party, called the proxy with knowledge of the decryption key of the data owner may be employed to handle this task. But the anonymity of the cipher-text receiver cannot be achieved as the data owner needs to know the information of recipient to proceed for re-encryption. Therefore, both of the approaches do not work well efficiently. So, Mambo and Okamoto introduced [5] and further defined in [2], Proxy Re-Encryption (PRE) to tackle the problem of data sharing by using a semi-trusted party called as the proxy that will be available at all times to handle the workload of the system. This work also concentrates on the identity-based cryptographic setting. To employ PRE in the IBE setting, [4] defined the concept of Identity-Based Proxy Re-Encryption (IBPRE), which offers a practical solution for access control in networked file storage [4], and secure email with IBE [4]. To provide privacy-preserving property and cipher-text's recipient update simultaneously, [6] an anonymous IBPRE system, which is CCA security model is proposed.

4. Detailed Approach

This paper aims to propose a cipher-text sharing mechanism using Proxy Re-Encryption with the following properties:
Anonymity: Nobody knows the identity information of sender and receiver for any cipher-text.
Multiple updates by receiver: The receiver of the cipher-text can be updated in multiple times.
Multi-sharing control: A cipher-text can be fine-grained shared with others if some pre-defined conditions are satisfied.

Security Models: The proposed scheme has four security models for IB-PRE and CCA notions:

- The security model of IB-PRE is the basic one, in which a data owner launches Chosen-Cipher-text Attacks (CCA) to the original cipher-text and re-encrypted cipher-text.
- The second case considered here is where a proxy colludes with sender to compromise the underlying message and the secret key of receiver. Security for the message is very difficult to provide as the sender can decrypt the cipher-text for the proxy. But the secret key of the receiver is very secure.
- In collusion attacks model, an intruder can acquire all re-encryption keys, and an intruder encrypts the data if it outputs a valid secret key of an uncorrupted user.
- For the security model of anonymity, anonymity should be given to both the sender and the receiver. This means that the original cipher-text should not output the identity of the sender and the receiver. The second anonymity is for re-encryption keys. This means that the intruder cannot distinguish between valid and a random re-encryption key.

Combining the above four models a unidirectional Anonymous Multi-Hop Identity-Based Conditional Proxy Re-Encryption (AMH-IBCPRE) is proposed, to achieve Anonymity, Multiple

updates by receiver and Multiple-sharing control simultaneously. The functionality of the system is described in Fig. 1. This scheme is applicable to many real-world applications, such as secure email forwarding and electronic encrypted data sharing. In the multiple receiver update scenario, Green and Ateniese [4] proposed the first MH-IBPRE scheme with CPA security. However, this scheme is not collusion-safe. Hence, to solve this problem, Shao and Cao [7] proposed a CCA-secure MH-IBPRE in the standard model which has the collusion-safe property. Hiding the information leaked from the re-encryption was defined by Ateniese et al. [8] using a notion called as key-privacy where the intruder cannot identify both the sender and the receiver even if the proxy key is provided. This model was later revised by Shao et al. [9]. Emura et al. [10] proposed a unidirectional IBPRE scheme in which an intruder cannot identify the source from the destination cipher-text which prevents the cipher-text from being traced. Finally, to ensure the privacy of both sender and receiver, Shao et al. [11] proposed the first Anonymous PRE (ANO-PRE) system, which guarantees that an intruder cannot identify the recipient of original and re-encrypted cipher-text for any proxy key. The first anonymous IBPRE with CCA security model was proposed in 2012 by Shao [6]. Comparing the proposed scheme with the existing systems, the comparison between the properties is summarized in table 1. Properties such as multiple cipher-text receiver update (denoting as M.U.), conditional share, collusion resistance (denoting as C.R.), anonymity, and without random oracle (denoting as W.R.O.) have been partially achieved by previous schemes, but there is no effective CCA-secure proposal that achieves all properties simultaneously in the standard model. This proposed mechanism for the first time, tries to fill the gap.

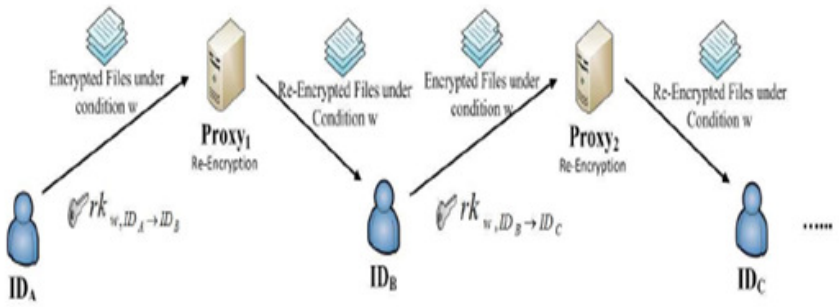

Fig. 1. Anonymous Multi-Hop Identity-Based Conditional Proxy Re-Encryption.

Table 1: Functionality and Security Comparison

Security	W.R.O.	M.U.	C.R.	Conditional Share	Anonymity
CPA	No	Yes	No	No	No
RCCA	Yes	Yes	No	No	No
CCA	No	Yes	Yes	No	No
CCA	Yes	No	Yes	No	Yes
CCA	Yes	Yes	Yes	Yes	Yes

System Construction: A unidirectional Multi-Hop Identity-Based Conditional Proxy Re-Encryption (MH-IBCPRE) scheme consists of the following algorithm:

a) *Generate master private and secret key*: KeyGen(mpk,msk)←Setup(k): Here k is the password. Output a master private key and a master secret key.
b) *Input the data for encryption*: Input(mpk,m):Input a delegator's message m, corresponding private key mpk.

c) *1-level cipher-text*: c1←Enc(m): Encrypt delegator's message m, output a 1- level cipher-text c1.
d) *l-level cipher-text*: c(l+1)←ReEnc)c1,msk,ID): On input of 1-level cipher-text c1 and corresponding secret key msk, output an l-level cipher-text under the delegate's identity ID, where $l > 1, l \in N$
e) *Decrypting l+1 cipher-text*: m←Dec (msk,mpk,Cl+1): On input msk, mpk and an l+1 level cipher-text under the delegate's identity ID. Output a message m or unsuccessful for failure.

5. Conclusion

In recent years, the need for security and privacy in big data storage services has been a major problem for the users of big data. The basic need is to ensure the privacy of the data and the anonymity of the service clients simultaneously. Additionally, the system should also provide a method where encrypted data is shared by the data owner among the various data users under some pre-defined conditions. Hence, this paper proposes a privacy preserving cipher text multi-sharing mechanism to achieve the above properties. This mechanism combines the merits of proxy re-encryption with anonymous technique in which a cipher-text can be securely and conditionally shared multiple times without leaking both the knowledge of underlying message and the identity information of cipher-text senders/recipients.

References

[1] K Liang, W Susilo, & JK Liu. Privacy-Preserving Cipher-text Multi-Sharing Control for Big Data Storage.
[2] M Blaze, G Bleumer, & M Strauss. (1998). Divertible protocols and atomic proxy cryptography. *In: Advances in Cryptology*. Berlin, Germany: Springer-Verlag. pp. 127–144.
[3] Y Dodis, & A Ivan. (2003). Proxy cryptography revisited. *In:* Proceedings of the 10th Network and Distributed System Security Symposium, February 2003.
[4] M Green, & G Ateniese. (2007). Identity-based proxy re-encryption. *Applied Cryptography and Network Security (LNCS)*. Vol. 4521. Berlin: Springer-Verlag. pp. 288–306.
[5] M Mambo, & E Okamoto. (1997). Proxy cryptosystems: Delegation of the power to decrypt ciphertexts. *IEICE Trans. Fundam. Elec. Commun. Comput. Sci.*, Vol. E80-A, No. 1, pp.54-63.
[6] J Shao. (2012). Anonymous ID-based proxy re-encryption. *Information Security and Privacy (Lecture Notes in Computer Science)*. Vol. 7372. Berlin: Springer-Verlag, pp. 364–375.
[7] J Shao, & Z Cao. (2012). Multi-use unidirectional identity-based proxy re-encryption from hierarchical identity-based encryption. *Inf. Sci*., Vol. 206, pp. 83–95.
[8] G Ateniese, K Benson, & S Hohenberger. (2009). Key-private proxy re-encryption. *Topics in Cryptology–CT-RSA (LNCS)*. Vol.5473. Berlin: Springer-Verlag, pp. 279–294.
[9] J Shao, P Liu, & Y Zhou. (2011). Achieving key privacy without losing CCA security in proxy re-encryption. *J. Syst. Softw*. 85(3), pp. 655–665. Available: http://doi:10.1016/j.jss.2011.09.034
[10] K Emura, A Miyaji, & K Omote. (2011). An identity-based proxy re-encryption scheme with source hiding property, and its application to a mailing-list system. *Public Key Infrastructures, Services and Applications (LNCS)*. Vol. 6711. Berlin: Springer-Verlag, pp. 77–92.
[11] J Shao, P Liu, G Wei, & Y Ling. (2012). Anonymous proxy re-encryption. *Secur. Commun. Netw*. 5(5), pp.439–449.