International Journal of Computer Applications (0975 - 8887)
Volume 164 - No.5, April 2017

Proxy Re-encryption Schemes for Secure Cloud Data and Applications: A Survey

Raghi Roy
PG Student
Department of Computer Science & Engineering
Fisat Engineering College
Angamaly, Ernakulam, India

Paul P. Mathai
Assistant Professor
Department of Computer Science & Engineering
Fisat Engineering College
Angamaly, Ernakulam, India

ABSTRACT

This paper presents a survey on Proxy re-encryption techniques with respect to secure cloud data and its application. To keep sensitive user data confidential against untrusted servers, cryptographic methods are used to provide security and access control in clouds. As the data is shared over the network, it is needed to be encrypted. There are many encryption schemes that provide security and access control over the network.Proxy re-encryption enables the semi-trusted proxy server to re-encrypt the ciphertext encrypted under Alice's public key to another ciphertext encrypted under Bob's public key. The re-encryption is done without the server being able to decrypt the ciphertext.Cloud services and applications should follow the standard security measures including data confidentiality, integrity,privacy, robustness and access control.In this paper the proxy re-encryption(PRE) schemes, Conditional PRE,Identity based PRE and Broadcast PRE,Type based PRE, Key private PRE,Attribute based PRE,Threshold PRE and its role in securing the cloud data are explained.

Keywords

Proxy re-encryprion,cloud storage,data confidentiality

1. INTRODUCTION

Cloud computing is emerging as a inevitable option for internet based applications and services. Cloud computing is a distributed computing architecture where the computing resources such as hardware, software, processing power are delivered as a service over a network infrastructure. The cloud computing model allows the users to access information and other resources from anywhere that a network connection is available[1].

In cloud computing all data are stored on distributed servers at remote location. The remote locations are data centres. The client can purchase or rent, such as handling time, network bandwidth, disk storage and memory[2]. Data owners can remotely store their data in the cloud and no longer posses the data locally. Cloud computing migrates the application software and database to the large data centre, where the data management and services may not fully trustworthy [4].

A cloud storage system is a distributed storage system [3] that consists of many independent storage servers. The function of distributed storage systems is to store data confidentially and reliable over long periods of time [6]. The main reason for the raise of the technology cloud computing is because of the convenience that they provide to different newly developed applications and for enterprises . The information that are stored in the cloud is been accessed a huge number of times and is often subjected to changes. An important aspect of cloud storage servers is that, it gives rise to a number of security threats.

Cloud services and applications may require all standard security functions including data confidentiality, integrity, privacy, robustness and access control. Hence securing the could and its data is a challenging task. There are several cryptographic methods to secure the data stored in cloud storage systems. Proxy re-encryption is a relatively new data encryption technique devised primarily for distributed data and file security.The target of proxy re-encryption is allowing the re-encryption of one cipher text to another cipher text without relying or trusting the third party that performs the transfer. In situations where one user wishes for another user to decrypt a message using its own or a new secret key instead of the first user's secret key, one technique involves the assistance of a proxy.

Proxy re-encryption[8] is a means for confidential and flexible technique for a user to store and share data. A user can encrypt the file with a public key and then store the ciphertext in a trusted server.When a receiver arrives, the sender can delegate a re-encryption key associated with the particular receiver to the trusted server as a proxy.Then the proxy re-encrypt the initial ciphertext to the desired receiver.The purpose of proxy re-encryption schemes is to prevent the revelation of the keys involved in re-encryption and the plaintext that needs to be re-encrypted to the proxy.

The Proxy re-encryption schemes are basically a version of existing encryption schemes consisting of selection of text, generation of keys, sharing or transmitting of keys between the parties, changeover from plaintext to cipher-text on one end and changeover from cipher-text to plaintext on the other end, the difference arises with the introduction of two more properties Directionality and Transitivity.

Directionality

If the re-encryption scheme is reversible that is, the same re-encryption key is used to translate messages from Alice to Bob, as well as from Bob to Alice the scheme is classified as a bi-directional

scheme. In these schemes if a user forwards a message to another, it automatically gives rights to the receiver to communicate with the sender. Such re-encryption keys are hence generated with the keys in hands of both sender and receiver and with their mutual trust and consent.

A unidirectional scheme is one-way in this context, giving a higher level of security and making it a feasible option in non trusted setups where message conveying is essential but not to an extent where receiver should be given rights to respond to it. So if a message is re-encrypted from Alice to Bob with a key, it cannot be used for re-encryption from Bob to Alice. Moreover uni-directional schemes are more useful since they can be converted to bidirectional scheme at any time simply by running it in both directions, i.e. from Alice to Bob and from Bob to Alice[9].

Transitivity:

Transitivity in proxy re-encryption schemes is defined as the number of re-encryptions allowed by an algorithm. A transitive PRE scheme would allow a cipher text to be re-encrypted from Alice to Bob, and then again from Bob to Tom and so on. While a non-transitive scheme would allow a cipher text to be re-encrypted for a single time (or a pre-defined limited number). This implies that inn non-transitive schemes the proxy does not have the authority to assign delegation rights to others beside the pair of communicating users.

In this paper encryption technique proxy re-encryption (PRE) scheme and its different categories such as Type based PRE,Key-private PRE, Identity based PRE, Attribute based PRE and Threshold PRE are discussed in the following section along with its role in cloud applications.

2. PROXY RE-ENCRYPTION SCHEMES

The proxy re-encryption schemes are proposed by Mambo and Okamoto [5] and Blaze et al. [8]. Proxy re-encryption is a cryptographic primitive which translates ciphertexts from one encryption key to another encryption key. It can be used to forward encrypted messages without having to expose the cleartexts to the potential users. The re-encryption protocol should be key independent to avoid compromising the private keys of the sender and the recipient. The primary advantage of this PRE [10] scheme is that they are unidirectional (i.e., Alice can delegate to Bob without Bob having to delegate to her) and do not require delegators to reveal their entire secret key to anyone.

Based on these properties many PRE techniques was proposed in the traditional public key infrastructure accompanied with much more sophisticated certificate management.Proxy Re-encryption can be broadly classified into two categories.They are (a)Uni-Directional Schemes and (b) Bi-Directional Schemes.

The Uni-Directional Schemes are further classified as (a)Identity-based PRE, (b)Attribute Based PRE, (c)Ciphertext-Policy Attribute based PRE,(d)Conditional PRE, (e)Time based PRE. The Bi-Directional Schemes are further classified as (a)Type based PRE and (b)Thershold based PRE

2.1 Type Based Proxy Re-encryption Scheme

[6] proposed the Type based proxy re-encryption scheme. This encryption scheme guarantees data confidentiality and fine gain access control. Type based PRE enables the delegator to implement fine grained policies with one key pair without any additional trust on the proxy.

The messages are categorized into different types according to the decryption rights of the intended receivers. The main benefit of this scheme is the single pair of keys which provides re-encryption capability to the proxy for his cipher-texts against his receivers. But the proposed scheme works only for the cipher-texts generated by the sender.The Type Based PRE poses some properties such as:

—The delegator only needs one key pair so that key management problem can be simplified.
—The delegator can choose a particular proxy for a specific delegate, which might be based on the sensitiveness of the delegation. Compromise of one proxy key will only affect one subset of messages.

2.2 Threshold Based Proxy Re-encryption Scheme

A fundamental approach of threshold PRE scheme [7] is for secure computation. This scheme performs huge number of computations on encrypted data without decrypting it. Threshold PRE technique has multiplicative homomorphic property.A multiplicative homomorphic encryption scheme supports the encoding operation over encrypted messages and forwarding operations over encrypted and encoded messages.

2.3 Identity-based Proxy Re-encryption Scheme

In Identity-based PRE(IB-PRE) schemes proposed by Ateniese in [1], in which senders encrypt messages using the recipients identity (a string) as the public key.An Identity-Based Proxy Re-encryption (IB-PRE) scheme is an extended Identity Based Encryption scheme.The identity-based proxy re-encryption (IB-PRE) schemes allow a proxy to translate an encryption under Alice's identity into one computed under Bob's identity. The proxy uses proxy keys, or re-encryption keys, to perform the translation without being able to learn the plaintext. Moreover, no information on the secret keys of Alice and Bob can be deduced from the proxy keys.

Both PRE and IB-PRE is confined to single receiver. In case of multiple receivers then the particular system is forced to use PRE or IB-PRE multiple times.Hence to get out of this issue, the idea of broadcast PRE(BPRE) was introduced [10].BPRE which runs the system in same as the PRE and IB-PRE but in a much more satisfying manner.

2.4 Key Private Proxy Re-encryption Scheme

Key private proxy re-encryption scheme are proposed by Ateniese et al. [11]. In a KP-PRE it is quite hectic task for the proxy and a set of colluding users to get the recipient of a message from the ciphertext and the set of public keys. Achieving key private PRE can only happen when the encryption scheme used is key-private. The key privacy encryption provides privacy of the key under which the particular encryption was performed.

The KP-PRE scheme gave raise to the idea of key privacy for proxy re-encryption schemes, where even the proxy who performs the particular translations cannot be able to distinguish the identities of the participants. In addition to hide the contents of files from the proxy, it is also useful to suppress as much meta-data as possible. For example, we might want the proxy file server to re-encrypt sensitive files for certain recipients without the proxy the recipient's identity.

2.5 Attribute Based PRE

In attribute based proxy re-encryption scheme [16], a semi trusted proxy with some additional information can transform a ciphertext under a set of attributes into a new ciphertext under another set of attributes on the same message. This encryption scheme, allows fine-grained access control on encrypted data. Attribute based encryption is a generalized form of IBE.Two types of attribute based encryption (ABE) namely ciphertext policy attribute based encryption (CP-ABE) and key policy attribute based encryption (KP-ABE).

Ciphertext Policy Attribute-Based PRE provides a fine grained access control over data by limiting the decryption rights based on some attributes of the receiver but it has an average efficiency and flexibility compared to the other schemes.CP-ABE is more apt for an enterprise environment, and it is an ideal unique scheme for implementing a self-contained data protection mechanism.

In KP-ABE [16] scheme, each ciphertext is named by the encryptor with a set of descriptive attributes. Each private key is held with an access scheme that mentions which type of ciphertexts the key can be used to decrypt. An important area of KP-PRE scheme deals with is in the field of secure forensic analysis.

2.6 Conditional PRE

Proxy re-encryption can be used in applications where delegation is required, for an example in case of delegated email processing. But, it is not enough to handle scenarios where a fine-grained delegation is demanded. For example, john is only allowed Lisa's encrypted emails containing a predetermine keyword. In order to overcome the limitation of existing PRE, in [15] the system introduces the notion of conditional proxy re-encryption (or C-PRE), whereby only ciphertext satisfying one condition set by Alice can be transformed by the proxy and then decrypted by john. The author formulates its security model and also proposes an efficient C-PRE scheme, whose chosen-ciphertext security is proven under the 3-quotient bilinear Diffe-Hellman assumption. The author further extends the structure, which allows multiple conditions with a somewhat high overhead.

2.7 Time based PRE

Time based PRE is a more recent updated scheme of PRE schemes which provides a scalable user revocation and reduces the workload of data owners. The major disadvantage of this scheme is that it requires the effective time period to be same for all attributes associated with the user.In this case, the data owner can be offline in the process of user revocations. The main idea is to combine the concept of time together with Attribute based encryption (ABE) and Proxy re-encryption (PRE). In time PRE scheme, the data is held with an attribute based access structure and an access time. Each user is identified by a set of attributes and a set of eligible time periods which denote the period of validity of user's access right. The scheme allows every user's access right to be effectual in a pre-determined time period, and enables the cloud service provider(CSP) to re-encrypt ciphertexts eventually, based on their own time.

3. LITERATURE SURVEY

Cloud service providers finds out the access control mechanisms for data on the cloud. Access control is a method that restricts, denies, or allows access to system. In the cloud, data security is crucial to protect against inside attack, denial of service attack, and collision attack. Traditionally, different successful access control policies are used to protect data stored locally and data stored remotely.One of such approach is Proxy Re-encryption(PRE) technique.

In [5] a methodology for delegating decryption rights was first introduced as an efficiency improvement over traditional decrypt-and-then-encrypt approaches. The proxy re-encryption key, cloud server can transform the ciphertext encrypted under the public key of Alice into an encryption under the public key of Bob. By utilizing the PRE primitive, the transformed ciphertext can only be decrypted by Bob whereas the cloud server is unable to learn the plaintext or private keys of Alice or Bob. Finally, Bob can download and decrypt the requested data with his own private key. In this way, the costly burden of secure data sharing can be offloaded to the semi-trusted cloud server with abundant resources.

In 1998, Blaze, Bleumer, and Strauss [8] proposed the notion of "atomic proxy cryptography", in which a semi-trusted proxy computes a function that converts ciphertexts for Alice into ciphertexts for Bob without seeing the underlying plaintext.The authors noted, however, that this scheme contained an inherent restriction: it is bidirectional.Thus, this scheme is only useful when the trust relationship between Alice and Bob is mutual.Delegation in the BBS scheme is transitive, which means that the proxy alone can create delegation rights between two entities that have never agreed on this.Another drawback to this scheme is that if the proxy and Bob collude, they can recover her secret key.

Jakobsson [17] developed a quorum-based protocol where the proxy is divided into sub-components, each controlling a share of the re-encryption key; here, the keys of the delegator are safe as long as the proxies are honest. A similar approach was considered by Zhou, Mars, Schneider and Redz [18].

Ivan and Dodis [19] realized unidirectional proxy encryption for El Gamal, RSA, and an IBE scheme by sharing the user's secret key between two users. They also solved the issue regarding the proxy alone assigning new delegation rights.One exception is the Ivan-Dodis IBE scheme [19] where the global secret that decrypts all ciphertexts is shared between the proxy and the delegatee. Thus, the delegatee need only to take care of a single secret, but an obvious drawback is that when the proxy and any delegatee in the system collude, they can decrypt everyone else's messages.

Apart from the generic construction of Dodis and Ivan there are two identity-based proxy re encryption schemes: one is proposed by Green and Ateniese [9] and the other is proposed by Matsuo [21]. In both schemes, the delegator and the delegatee are assumed to be registered at the same domain (or, the same key generation center).The IBE has a number of practical applications such as secure email forwarding, attribute-based delegations and access control in networked file storage. This type of re-encryption schemes is utilised to realize the secrecy of data.

Sahai and Waters in [20] introduced the first attribute-based encryption (ABE) where both the ciphertext and the secret key are labelled with a set of attributes. A user can decrypt a ciphertext only if there is a match between the attributes listed in the ciphertext and the attributes with in hand of the decryptor. ABE schemes can be classified into two types: key-policy ABE (KPABE) and ciphertext-policy ABE (CP-ABE).

In ABE technique, the data is stored on the storage server in an encrypted form while different users are still allowed to decrypt different pieces of data as per security policy. This successfully eliminates the need to rely on the storage server for preventing unauthorized data access.

Jean Weng in [10] introduced Conditional proxy re-encryption (C-PRE),the proxy is unable to translate those ciphertext whose corresponding condition keys are not available.However, proxy will obtain no information about the original message. The security requirements for C-PRE systems should ensure that, (i) even if the proxy, who does not have both the partial re-encryption key and the condition key, conspire with the delegate, it is still impossible for them to compromise the delegator's security. (ii) The proxy, who has both the partial reencryption key and the condition key, compromises neither the delegator not the delegatee's security.

To employ PRE in the context of TRE(Timed Release Encryption), Emura et al.[22] proposed the first Timed-Release Proxy Re-Encryption (TR-PRE).In TR-PRE, the proxy is allowed to re-encrypt a ciphertext with a release time under a public key to the one with the same release time under another public key by using a re-encryption key given by the delegator.

Conditional Proxy Broadcast Re-Encryption (CPBRE), which was proposed by Chu et al. [15], can further reduce the cost incurred by TR-PRE. Specifically, CPBRE allows a delegator to delegate the decryption rights of a broadcast encryption to a set of delegatees, and to specify a condition to control the re-encryption power of the proxy.

The main intention of cloud storage system is to secure the data itself in such a way that even in the event of a successful attack. The content of the data stored in the cloud storage system remains confidential and secureed. To provide confidentiality for messages in storage servers, a user can encrypt messages by a cryptographic method to encode and store messages.

4. COMPARISON OF PRE SCHEMES

in this section we compare different proxy re-encryption techniques on the bases of the properties advantages and disadvantages.The comparison is compressed and represented in Table 1.

5. SECURE CLOUD DATA AND APPLICATIONS

What is the cloud? In general, the cloud is the concept of remotely hosted IT services, termed cloud apps, provided by a supplier. These suppliers are called cloud providers. Typical cloud apps offered by cloud providers include email, calendar, documents, online storage, sales, customer service, and more. Some of today's well known cloud providers include companies such as Amazon, Google, Intuit, Microsoft, and Box. A selection of the top cloud apps in the market today include Cloud Drive, Google Apps for Business, Skype,Quickbase and Box Business.

Using business apps in the cloud has widely recognized advantages: you save money by paying for only the IT computing resources you need, you can use the computing resources quickly without capital investment, and you can increase your reach to employees and users anywhere.Some areas of application of cloud computing are:

Personal Health Record:"An electronic, lifelong resource of health information needed by individuals to make health decisions". PHR acts as an important intermediary between physicians and patients. The main goal of PHRS is to enable patients to manage and maintain their personal health records as well as improving healthcare delivery and reducing cost.Security and privacy are the main concern for patients in regard to their health records.By using proper cryptographic encryption techniques the PHR can be secured by the individuals.The right of disclosing the details will be with in the particular individual.This mode of protection of data is necessary as the disclosure of health details at certain situation can cause a negative impact on the person such during a job interview,insurance etc.

Data Sharing in Cloud Computing: Despite the abundant resource provided by the cloud computing, data owners' concerns about the privacy of their outsourced data such that these data can only be accessed by the authorized parties become the main obstacles impede cloud computing from spread adoption, especially if the cloud server is only semi-trusted.proxy re-encryption is a promising candidate to enable secure data sharing in the cloud computing.

Encrypted Email Forwarding: By utilizing the PRE primitive in a encryption email system, the granted recipient first generates a re-encryption key using his own private key and the delegatee's public key, and delegates this key to a email server. Then relying on the PRE scheme the email server can achieve transformations from the recipient's encrypted emails into the delegatee's encrypted emails without disclosing any information.Finally, the delegatee can check the delegator's encrypted emails conveniently with his own private key. Crucially, the private key for the recipient is protected from being disclosed in this email system.

Digital Rights Management: The digital rights management (DRM) is developed to prevent digital contents from being copied and redistributed illegally by binding a digital content and a unique license together.In order to achieve inter-operability among different DRM systems, some primitive of PRE was introduced into DRM.

Vehicular Ad Hoc Networks: By enabling vehicles to communicate with other vehicles or roadside units (RSUs) via the equipped on-board units (OBUs) communication devices, vehicular ad hoc networks (VANETs) can be formed to offer a more efficient and comfortable driving experience.VANETs can be formed to offer a more efficient and comfortable driving experience.To address the trust and privacy issues in VANETs,an authentication protocol with privacy preservation by incorporating appropriate proxy re-encryption schemes.In their authentication protocol, the RSU is able to transform a signature from a OBU into another signature from TA on the traffic message without revealing any private information of the OBU. This conceals the real identity of the OBU from malicious adversary.

6. CONCLUSION

In cloud computing,security is an important step in quality of service. To keep the sensitive and trustworthy user data confidential against untrusted servers several proxy re-encryption techniques are used.PRE has captured a lot of concern due to the delegation function of decryption.PRE is also an essential technique as many real time applications and many big and small ventures relay on cloud based storage for storing the sensitive data concerning them.

This paper surveys different proxy re-encryption schemes used in cloud storage system. The advantages and disadvantages of the schemes have been studied and summaries for future use. The future work will be concerned with:

Table 1. Comparative study of Proxy Re-encryption Techniques.

PRE Schemes	Key Features	Advantages	Disadvantages
PRE	Directionality and Transitivity	PRE is secure against plain text attack	Collusion problem and Plaintext attack
TB-PRE	Non-Interactive,Key-private,Ciphertext-private	Semantic security and Ciphertext Privacy Control	Encoding operations over encrypted messages is not possible
KP-PRE	Non-Interactive,Unidirectional,Key-private,Collusion-resistant,Ciphertext-private	Provides CCA security	The key privacy proof is more difficult than that of CPA security
IB-PRE	Multiple-use,Non-Interactive,Ciphertext-private	Secure against an adaptive chosen Ciphertext attack	Difficult to find efficient constructions for multiuse CCA-secure IBEPRE.
AB-PRE	Uni-directional,Multiple-use,Non-Interactive,Collusion-resistant,Ciphertext-private	Fine-grained access control on encrypted data	Average efficiency and flexibility
C-PRE	Uni-directional,Non-Interactive,Collusion-resistant,Ciphertext-private	Security against chosen Ciphertext attack	It is difficult to design CCA secure C-PRE scheme
T-PRE	Bi-Directional,Collusion-resistant,Ciphertext-private	Data Forwarding	High access control

—the development of better PRE schemes which works in distributed environment.

—finding the efficient PRE schemes with full security is also an open problem since most of the existing PRE schemes can only achieve certain selective security.

7. REFERENCES

[1] Giuseppe Ateniese, Kevin Fu, Matthew Green, and Susan Hohenberger. Improved proxy re-encryption schemes with applications to secure distributed storage, *In Proceedings of the 12th Annual Network and Distributed System Security Symposium* , pages 29-44. Internet Society, February 2005.

[2] A. G. Dimakis, P. G. Godfrey, Y. Wu, M. J. Wainwright, and K. Ramchandran, *Network coding for distributed storage systems*,IEEE, 2010,pp. 4539-4551.

[3] P. Druschel and A. Rowstron,*PAST: A Large- Scale, Persistent Peer-to-Peer Storage Utility*, Proc.Eighth Workshop Hot Topics in Operating System, 2001, pp. 75-80.

[4] C.Wang, QianWang, KuiRen, and Wenjing Lou, *Ensuring Data Storage Security in Cloud Computing*, Proc. IWQoS 09, July 2009, pp. 1-9.

[5] M. Mambo and E. Okamoto,*Proxy Cryptosystems: Delegation of the Power to Decrypt Ciphertexts*, IEICE Trans. Fundamentals of Electronics, Comm. and Computer Sciences, 1997, pp. 54-63.

[6] Q. Tang, *Type-Based Proxy Re-Encryption and Its Construction*, Proc. Ninth International Conf. Cryptology in India, 2008, pp. 130-144.

[7] S. Saduqulla and S. Karimulla, *Threshold Proxy Re-Encryption in Cloud Storage System*, International Journal of Advanced Research in Computer Science and Software Engineering,Volume 3, Issue 11, November 2013.

[8] M. Blaze, G. Bleumer, and M. Strauss, *Divertible Protocols and Atomic Proxy Cryptography* in Proc. Int. Conf. Theory Appl. Crytographic Techn.: Adv. Cryptol, (1998)127-144.

[9] M. Green and G. Ateniese, *Identity-based proxy re-encryption*, in Proc. 5th Int. Conf. Appl. Cryptography Netw. Security, 2007, pp. 288-306.

[10] C.-K. Chu, J. Weng, S. S. M. Chow, J. Zhou, and R. H. Deng, *Conditional proxy broadcast re-encryption*,in Proc. 14th Australasian Conf. Inf. Security Privacy, 2009, pp. 327-342.

[11] G. Ateniese, K. Benson and S. Hohenberger, Key-Private Proxy Re-Encryption, *Topics in Cryptology, Springer*, 2009.

[12] Jian Weng, Robert H. Deng, Xuhua Ding, Cheng- Kang Chu, and Junzuo Lai,*Conditional proxy reencryption secure against chosen-ciphertext attack*,In ASIACCS ,2009,pp. 322-332.

[13] Rutuja Warhade,Prof. Basha Vankudothu, *A Survey on Proxy Re-encryption Schemes for Data Security in Cloud* International Journal of Advance Research in Computer Science and Management Studies,12,(2014)

[14] A. Boldyreva, M. Fischlin, A. Palacio, and B. Warinschi,*A closer look at PKI: Security and efficiency*, in Proc. 10th Int. Conf. Practice Theory Public-Key Cryptography, (2007)458-475.

[15] Jian Weng, Robert H. Deng, Xuhua Ding, Cheng- Kang Chu, and Junzuo Lai, *Conditional proxy reencryption secure against chosen-ciphertext attack*,In ASIACCS,2009,pp. 322-332.

[16] Goyal V, Pandey O, Sahai A, and Waters B ,*Attribute Based Encryption for Fine-Grained Access Conrol of Encrypted Data*,In: ACM conference on Computer and Communications Security, 2006.

[17] Markus Jakobsson, *On quorum controlled asymmetric proxy re-encryption*, In Proceedings of Public Key Cryptography, pages 112-121, 1999.

[18] Lidong Zhou, Michael A. Marsh, Fred B. Schneider, and Anna Redz, *Distributed blinding for ElGamal re-encryption*,Cornell Computer Science Department, 2004.

[19] Yevgeniy Dodis and Anca Ivan,*Proxy cryptography revisited*,In Proceedings of the Tenth Network and Distributed System Security Symposium, February 2003.

[20] A. Sahai and B. Waters,*Fuzzy identity-based encryption*, in Proc. EUROCRYPT 05, vol. 3494 of Lecture Notes in Computer Science, Springer, Heidelberg, pp. 457-473, 2005.

[21] T. Matsuo *Proxy re-encryption systems for identity-based encryption*, In T. Takagi, T. Okamoto, E. Okamoto, and T. Okamoto, editors,pp. 457-473,

[22] Emura, K., Miyaji, A., Omote, *A timed-release proxy re-encryption scheme* IEICE Transactions,98-A(8), 16821695 (2011)