IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 9, Issue 10, October 2020

DOI 10.17148/IJARCCE.2020.91022

A study on Proxy Re-Encryption Schemes

Shashank Shekhar Tiwari[1], Hemant Kumar Baranwal[1], Shweta Tiwari[1], Ritika Yaduvanshi[2]

Department of Information Technology, Rajkiya Engineering College Ambedkar Nagar (U.P), India[1]

Department of Computer Science and Engineering, Mahamaya College of Agricultural Engineering and Technology, Akbarpur, Ambedkar Nagar (U.P), India[2]

Abstract: Proxy Re-Encryption (PRE) is now a primitive encryption used to assign decryption privileges. It was introduced by Blaze, Bleumer and Strauss. With the use of a proxy agent, PRE enables re-encryption of a ciphertext intended for one party to a ciphertext for another party. The underlying message and the sender's private key cannot be read by the proxy agent. The properties of proxy re-encryption systems with different classifications of proxy re-encryption schemes are discussed in this paper.

Keywords: Directionality, Distributed System, Encryption, Proxy re-encryption, Transitivity

I. INTRODUCTION

Encryption is a way to secure our data from unauthorized person. Proxy re-encryption helps in file security and distributed storage. The purpose of this technique is allowing re-encryption of one cipher text to another ciphertext. The encryption is done using private or public key for securing data and perform authentication via sharing security key. In situation where one user wants for another user to decrypt the message by using its own key or a new secret key instead of first user's secret key. An easily implemented re-encryption scheme is one of the proxy in which proxy given control of both User's key so the message will converted into plaintext and re-encrypted for another user or second user. User1's secret key used to decrypt the message from cipher-text into plaintext whereas User2's secret key used to encrypt it.

However, this is the rebelling against the primary goal of security; the goal of the proxy re-encryption is to prevent the disclosure of keys that involves in re-encryption and the plaintext that needs to be re-encrypted to the proxy. In this context, the above method mentioned is not ideal. So for a scenario where belief cannot be held in a proxy. The requirement here is to convert messages encrypted on behalf of User1's public key to messages encrypted on behalf of User2's public key without the proxy being free to decrypt the message. The scheme that ensure this action known as proxy Re-encryption. After all proxy re-encryption scheme is generally, a version of existing encryption scheme found to choose text, generation of keys, transmitting the keys between the concerns parties, conversion from plaintext to cipher-text on one side and conversion from ciphertext into plaintext on another side, the difference appears with the introduction or foundation of two more properties given bellow [1, 2,14]:

A. *Directionality*

Re-encryption scheme categorized as bi-directional and uni-directional scheme. If the re-encryption scheme is reversible then the same re-encryption key is used to convert the messages from User1 to User2 and vice-versa, this scheme is categorized as bi-directional scheme. In which if user sends the message to another, it automatically provides rights to communicate with the sender. In this case, the re-encryption keys are generated with the keys of both sender as well as receiver with their mutual trust and agreements.

A uni-directional scheme is defined as one way scheme in this scenario, giving a higher level of security and make it feasible in non-trusted setups where message transmission is important but not to an extent where receiver should be given authority to respond to it. So if a message is re-encrypted from User1 to User2 with a key and that is not possible the same message is used for re-encryption from User2 to User1. Uni-directional scheme are more useful and can be converted into bi-directional scheme at any time as easily by running in both directions [12].

B. *Transitivity*

Transitivity is defined as the number of re-encryptions allowed by an algorithm in proxy re-encryption scheme (PRE). A transitive PRE would allow a cipher text to be re-encrypted from User1 to User2 and again User2 to User3 and keeps on. While a non-transitive PRE do not allow to a cipher text to be re-encrypted more than one time but only once (or pre-defined limited times). This means in non-transitive scheme proxy does not have authority to appoint deputation rights to others besides the pair of communicating users. Besides the previous mentioned properties, some more of the security properties proved by existing proxy re-encryption scheme are the disability of proxy to see plaintext apart from the scheme. The secret key generated at the end of the owner, and proxy in no way can determine the secret key of sender and receiver from the re-encryption key.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 9, Issue 10, October 2020
DOI 10.17148/IJARCCE.2020.91022

The transitivity and deputation level of applied scheme hang on the trust matrix of the involved parties (security, confidentiality, integrity, etc). The need of PRE scheme was first pointed up when Mambo and Okamoto in 1997 mentioned the concept of deputing decryption rights to improve the efficiency instead of the conventional decryption-and-then-encrypton approaches. Blaze, Bleumer, and Strauss (BBS) enhanced this experience in 1998 [4].When they proposed an application called atomic proxy re-encryption. In that proposed scheme a partially trusted proxy is permitted to perform conversion from a cipher-text for one user into another cipher-text for another user but cannot be permitted to access the highlighted plain-text. Even though efficiently computable, flexible and useful for selection of BBS re-encryption over a larger application domain for arranging encrypted file systems has been hindered by chosen security risk. These methods are still under progress of maturity and need fine-tuning before being adopted in every organization

II. CLASSIFICATION OF PROXY RE-ENCRYPTION

Proxy re-encryption schemes (PRE) are classified into the following two categories:

- Uni-directional Scheme
- Bi-directional Scheme

Unidirectional scheme are further classified as follow:

- Identity Based PRE
- Conditional PRE
- Ciphertext policy attribute based PRE
- Key private PRE
- Time based PRE

Bidirectional Scheme are classified as follows:

- Type based PRE
- Threshold PRE

A. *Identity and type based proxy re-encryption scheme:*

This scheme has highlighted the problem of multiple delegation of decryption rights. Assume that the delegator wants two different users to view different sub parts of his message. The solution will be to place trust in the proxy to re-encrypt the chosen parts of the cipher-texts using this method. This fails if the proxy is corrupted. A better but unrealistic alternative is selecting a different pair of keys for each delegate. This identity-based proxy re-encryption scheme is based on the Boneh Franklin Identity Based Encryption scheme enabling execution of different access control policies for cipher-texts against multiple receivers. The messages are classified into different types according to the decryption rules of the intended receivers. The main advantage of this scheme is the single pair of keys which provides re-encryption ability to the proxy for it's cipher-texts against it's receivers. But the suggested scheme works only for the cipher-texts generated by the sender. The method mentioned as follows:

Users classified their messages into different types Setup and Encryption are the same as in the Boneh Franklin scheme. Re-Encrypt (msg,type,msg_id) : the algorithm outputs the cipher-text 'sub_msg' = (msg1,msg2,msg3) based on the message and the type given by user. Every sub message is meant to be decrypted by the particular receiver and no one else. Decrypt (sub_msg, skid): Given a cipher-text 'sub_msg' = (msg1, msg2, msg3), the algorithm outputs the message 'msg' based on the 'skid' of the receiver. Hence every receiver gets the sub message calculated for him/her and nothing more [3,13].

B. *Condition Proxy Re-encryption Scheme*

In situation where fine-grained delegation is required requiring fulfilment of a predefined condition, the concept of conditional proxy re-encryption (or CPRE) was introduced, where by only cipher-text satisfying one condition set by Sender is permitted to be modified and then decrypted by receiver. The scheme is proven to be Chosen cipher text attack (CCA)-secured. The scheme is now upgraded to work based on multiple conditions rather than one, as was its beginning version. The conditions can be anything identified by the involved parties and the creation of the algorithm. They can be a set of pre-determined integers, the sending or receiving situation of the parties, the physical location of the sender or the receiver. The message to be transferred is encrypted using the receiver's public key and the condition. In similar fashion to decrypt the message the receiver should meet the predefined situations. The challenge now left to create CCA-secure C-PRE schemes with anonymous situation rather than known predefined conditions. [6].

C. *Based on Attribute Proxy Re-Encryption Scheme*

The Attribute based proxy re-encryption (A-PBE) schemes allocate a better option especially when replicating a user is in an active subject. Furthermore, the problem of authentication of a user is easily solved by this scheme. Attribute based PRE involves different user attributes like city, country, street , GPS parameters, or any other set of attributes that

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 9, Issue 10, October 2020
DOI 10.17148/IJARCCE.2020.91022

are predefined while encryption. When a user holds these attributes only then the decryption of a message is possible and permitted. The identification of these attributes is based on a fixed threshold i.e. if the attributes of the receiver matches the required attribute set by a certain degree or level, the decryption access is granted and the message can be decrypted by only using these attributes and the secret key. So that if a single attribute does not meet the threshold, the whole decryption fails. This is a common scheme whose various transformations exist, namely Cipher-Text policy attribute based encryption and Key policy attribute based encryption which are widely implemented. This mechanism is joined with the proxy re-encryption and implemented in different categories[10].

D. *Based on Key Private Proxy Re-encryption Scheme*

Key Private Proxy Re-Encryption also known as Anonymous Proxy Re-Encryption introduces the concept of keeping the keys private so that even the proxy that performs the modification of message cannot identify or differentiate between the involved users. This scheme is CPA-secure but work is still in improvement regarding CCA-safe key private PRE schemes. If a proxy communicates with many users it should not be able to disclose to a user, what other parties are communicating with it from the message being transmitted or the set of re-encryption keys available. This information should not guide to the users. The significance and benefit of a key private scheme is that nobody can detect who has access to a particular message i.e. complete anonymity of the user's part of communication. [7, 8]

E. *Based on Ciphertext-Policy Attribute Proxy Re-encryption(CP-ABPRE)*

Ciphertext-Policy ABPRE is a joint creation of attribute-based encryption and conventional proxy re-encryption scheme. It is proven secure against CPA. It is a type of ABE where the key is associated with an access structure namely a group of attributes explaining the type of user that should be given access and decryption rules. This solves the issue of multiple users and key distribution over a large scale. Key management creates an overhead in such situations and this algorithm is favorable in this context. Recent variations of this algorithm are proven secure against selected ciphertext attacks under decisional q-parallel BDH assumption. This algorithm has extensive applications in medical domains where patient records are continuously being transferred and referred from one doctor or facility to another. It provides a fine-grained access control to the user over the deputes enabling it to specify who can decipher the data or message by setting with it a set of attributes [9]. CP – ABPRE scheme is a conspiracy resistant uni-directional scheme and is connected with a monotonic access structure. A CCA secure version of CP-ABPRE is also created in [11].

F. *Based on Time Proxy Re-encryption Scheme*

A cloud environment is composed of several independent servers communicating to allocate services. In a time-based re-encryption scheme, each cloud server is allowed to independently re-encrypt data automatically in contrast to the previous scheme where the data was encrypted only after receiving a command from the sender. This permits an automatic re-encryption of data based on the internal time of the cloud servers rather than by manual commands. The data is associated with a control structure for determining access and a time for which the access is granted. So that every piece of data stored in the cloud is connected with a set of attributes that define the type of user the data is intended for and a time structure which primarily specifies the time limit for which the data will be accessible to the user[12].

The receiver is issued keys that become effective during the specified access times, implying that the receiver can decrypt the message using only those keys which match the access time. The secret key is shared by the data owner and cloud service provider. This key is used to create sub-keys for the users at later and when re-encrypting the data along with the clock time of the system. This composition of access structure facilitates user revocation and distribution of deputation rights. The algorithm is based on the Bilinear Deffie-Hellman assumption like most proxy re-encryption schemes. First the algorithm is setup by generating the master key, public key and describing a universal attribute set from which the individual attributes will be late selected. Then the Cloud Service Provider(CSP) identifies all its users and produces secret keys for them based on their attribute sets. The data is then encrypted based on the above described access structure. Now when a user requests for a certain data, it is re-encrypted with the internal time of the system, hence setting up a valid access time for decryption by the user. Hence user satisfying the access structure i.e. if the time has not expired then the attributes set can successfully attempt decryption [6, 15].

G. *Based on Threshold Proxy Re-encryption*

We get three problems in a decentralized cloud storage system. First, high level of traffic between the user and storage servers leads to more computation by the user. Second, key management becomes a problem for the user because security is broken if the user's keys are agreement. Thirdly, a user's messages directly forwarding to another one is not realistic. In Threshold Proxy Re-Encryption cloud storage stores user's details in database. The user needs to get registered in the database, by entering his data like user_name, user_gender, user_location and user_e-mail address. By

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 9, Issue 10, October 2020
DOI 10.17148/IJARCCE.2020.91022

using his credentials, the user then logs into the system. The file is transferred contained in a folder along with the user and recipients name, a question asks for security purpose, the file containing the key for decryption and the status of the message. The file is transferred using the receiver's email and public key. After the file is received by the receiver, the selected file is downloaded. But before downloading the file, he/she has to download the key file that was sent in the same folder. In order to download the key file, receiver has to enter the following details like file name, secure question and its answer. Now the key is revealed to the receiver with which the message can be downloaded and decrypted. [5]

III.COMPARATIVE STUDY

The following table1 shows the comparative analysis of PRE schemes discussed above:

TABLE I COMPARATIVE ANALYSIS OF PRE SCHEMES

S.N	Encryption Schemes	Directionality	Transitivity
1	Identity Based PRE	Uni directional	No
2	Conditional PRE	Uni directional	No
3	Ciphertext policy attribute Based PRE	Uni directional	No
4	Key private PRE	Uni directional	No
5	Time based PRE	Uni- directional	No
6	Type based PRE	Bi-directional	No
7	Threshold PRE	Bi-directional	No

IV.CONCLUSION

The various proxy re-encryption schemes have been mentioned in this complete scenario. These systems provide our data with protection and privacy that have directionality and transitivity properties, which provide an important encryption phenomenon.

REFERENCES

[1] M. Blaze, G. Bleumer and M. Strauss, Divertible protocols and atomic proxy cryptography, Proceedings of Eurocrypt '98, volume 1403, pages 127–144, 1998.
[2] Zhou, L., Marsh, M.A., Schneider, F.B., Redz, A.: Distributed blinding for ElGamal re-encryption. Technical Report 2004–1924, Cornell Computer Science Department (2004)
[3] Green, M., Ateniese, G.: Identity-based proxy re-encryption. Cryptology ePrint Archive, Report 2006/473 (2006)
[4] Blaze, M., Bleumer, G., Strauss, M.: Divertible protocols and atomic proxy Cryptography. In: Nyberg, K. (ed.) EUROCRYPT 1998. LNCS, vol. 1403, pp. 127–144. Springer, Heidelberg (1998)
[5] 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.
[6] Voltage Security, Inc., http://www.voltage.com
[7] A. Mrabet, N. El Mrabet, R. Lashermes, J.B. Rigaud, B. Bouallegue, S. Mesnager, M. Machhout, "A systolic hardware architectures of montgomery modular multiplication for public key cryptosystems", IACR CryptologyePrint Archive, pp. 487, 2016.
[8] G. Ateniese, K. Benson, S. Hohenberger, "Key-private proxy re-encryption", CT-RSA, pp. 279-294, 2009.
[9] Waters, B.: Efficient Identity-Based Encryption without random oracles. In: Proceedings of Eurocrypt '05. Volume 3494 of Lecture Notes in Computer Science., Springer (2005) 114–127
[10] Gilad Asharov, Abhishek Jain, Adriana Lopez-Alt,EranTromer,Vinod Vaikuntanathan,andDanielWichs, "Multiparty computation with low communication, computation and interaction via threshold FHE", Proceeding EUROCRYPT'12, Springer, 2012,pp. 483-501 Ian Foster,Yong Zhao, Ioan Raicu, and
[11] Shiyong Lu, "Cloud Computing and Grid Computing 360-Degree Compared", Grid computing workshop, 2008, pp.110.
[12] Qin Liu, Guojun Wang and Jie Wu, "Time-Based Proxy Re-encryption Scheme for Secure Data Sharing in a Cloud Environment", Information Sciences, In Press, 2012
[13] Shamir, A Identity-Based cryptosystem and signature schemes, Advances in Cryptology, pp. 47-53, 1984.
[14] Boneh, D., Di Crescenzo, G., Ostrovsky, R., Persiano, G.: Public key encryption with keyword search. In: Cachin, C., Camenisch, J.L. (eds.) EUROCRYPT 2004. LNCS, vol. 3027, pp. 506–522. Springer, Heidelberg (2004)
[15] Bhavya G, P. Ramachandran, Manasa V. and Srividhya V.R. Time Based Re-Encryption in Unreliable Clouds, International Conference on Advances in Computer