International Journal of Research
Available at https://edupediapublications.org/journals

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue 13
October 2017

A Survey On Cloud Email Based Conditional Identity-Based Broadcast Proxy Re-Encryption And Its Application

R.Mahesh & M. Venkatesh Naik

Assistant Professor[#1,2] *DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING*

Chiranjeevi Reddy Institute Of Engineering And Technology, Bellary Road, Anantapur, AP

ABSTRACT —*This Recently, variety of extended Proxy Re-Encryptions (PRE), e.g. Conditional (CPRE), identity-based PRE (IPRE) and broadcast PRE (BPRE), are projected for versatile applications. By incorporating CPRE, IPRE and BPRE, this paper proposes a flexible primitive noted as conditional identity-based broadcast PRE (CIBPRE) and formalizes its linguistics security. CIBPRE permits a sender to encode a message to multiple receivers by specifying these receivers' identities, and therefore the sender will delegate a re-encryption key to a proxy so he will convert the initial cipher-text into a replacement one to a replacement set of meant receivers. Moreover, the re-encryption key is related to a condition such solely the matching cipher-texts is re-encrypted, that permits the first sender to enforce access management over his remote cipher-texts in a very fine-grained manner. we tend to propose associate economical CIBPRE theme with obvious security. Within the instantiated theme, the initial cipher-text, the re-encrypted cipher-text and therefore the re-encryption key area unit dead constant size, and therefore the parameters to come up with a reencryption key area unit freelance of the first receivers of any initial cipher-text. Finally, we tend to show associate application of our CIBPRE to secure cloud email system advantageous over existing secure email systems supported Pretty sensible Privacy protocol or identity-based coding.*

Keywords - Proxy re-encryption, cloud storage, identity-based encryption, broadcast encryption, secure cloud email.

I. INTRODUCTION: Proxy re-encryption (PRE) [1] provides a secure and versatile method for a sender to store and share information. A user may code his file together with his own public key then store the cipher-text in AN honest-butcurious server. When the receiver is set, the sender will delegate a re-encryption key related to the receiver to the server as a proxy. Then the proxy re-encrypts the initial cipher-text to the intended receiver. Finally, the receiver will rewrite the resulting cipher-text together with her personal key. the protection of PRE typically assures that neither the server/proxy nor non-intended receivers will learn any helpful info about the (re-)encrypted file, and before receiving the re-encryption key, the proxy cannot re-encrypt the initial cipher-text during a meaty approach. Efforts are created to equip PRE with versatile capabilities. The early PRE was projected within the ancient public- key infrastructure setting that incurs difficult certificate management to alleviate from this downside, several identity-based PRE (IPRE) schemes were projected in order that the receivers' recognizable identities will function public keys. rather than taking and verifying the receivers' certificates, the sender and also the proxy just have to be compelled to recognize the receivers' identities, that is additional convenient in follow. PRE and IPRE permits one receiver. If there square measure a lot of receivers, the system must invoke PRE or IPRE multiple times. to deal with this issue, the construct of broadcast PRE (BPRE) has been planned [9]. BPRE works during a similar way as PRE and IPRE however a lot of versatile. In distinction, BPRE allows a sender to get AN initial ciphertext to a receiver set, rather than one receiver. Further, the sender will delegate a re-encryption key related to another receiver set so that the proxy will re-encrypt to. The on top of PRE schemes solely permits the re-encryption procedure is dead in AN all-or-nothing manner. The proxy will either re-encrypt all the initial cipher-texts or none of them. This coarse-gained management over cipher-texts to be re-encrypted could limit the appliance of PRE systems. To fill this gap, a refined construct stated as conditional PRE (CPRE) has been planned. In CPRE schemes a sender will enforce fine-grained re-encryption management over his initial cipher-texts. The sender achieves this goal by associating a condition with a re-encryption key. solely the ciphertexts meeting the required condition are often re-encrypted by the proxy holding the corresponding re-encryption key.

II. LITERATURE SURVEY

This paper proposes a new cryptographic primitive, named identity-based conditional proxy re-encryption (IBCPRE). In this primitive, a proxy with some information (a.k.a. re-encryption key) is allowed to transform a subset of cipher texts under an identity to other cipher texts under another identity. Due to the specific transformation, IBCPRE is very useful in encrypted email forwarding. Furthermore, we propose a concrete IBCPRE scheme based on Boneh-Franklin identity-based encryption. The proposed IBCPRE scheme is secure against the chosen cipher text and identity attack in the random oracle.

In this paper, for the first time, we define a general notion for proxy re-encryption (PRE), which we call deterministic finite automata-based functional PRE (DFA-based FPRE). Meanwhile, we propose the first and concrete DFA-based FPRE system, which adapts to our new notion. In our scheme, a message is encrypted in a cipher text associated with an arbitrary length index string, and a decryptor is legitimate if and only if a DFA associated with his/her secret key accepts the string. Furthermore, the above encryption is allowed to be transformed to another cipher text associated with a new string by a semi trusted proxy to whom a re-encryption key is given. Nevertheless, the proxy cannot gain access to the underlying plaintext. This new primitive can increase the flexibility of users to delegate their decryption rights to others. We also prove it as fully chosen-cipher text secure in the standard model.

III.PROBLEM DEFINITION

3.1 Existing System:

- ❖ PRE and IPRE allow a single receiver. If there are more receivers, the system needs to invoke PRE or IPRE multiple times. To address this issue, the concept of broadcast PRE (BPRE) has been proposed. BPRE works in a similar way as PRE and IPRE but more versatile.
- ❖ In contrast, BPRE allows a sender to generate an initial cipher text to a receiver set, instead of a single receiver. Further, the sender can delegate a re-encryption key associated with another receiver set so that the proxy can re-encrypt to.
- ❖ A recent conditional proxy broadcast re-encryption scheme allows the senders to control the time to re-encrypt their initial cipher texts. When a sender generates a re-encryption key to re-encrypt an initial cipher text, the sender needs to take the original receivers' identities of the initial cipher text as input. In practice, it means that the sender must locally remember the receivers' identities of all initial cipher texts. This requirement makes this scheme constrained for the memory-limited or mobile senders and efficient only for special applications.

Disadvantages of Existing System:

- ❖ The early PRE was proposed in the traditional public-key infrastructure setting which incurs complicated certificate management.
- ❖ The PRE schemes only allow data sharing in a coarse-grained manner. That is, if the user delegates a re-encryption key to the proxy, all cipher texts can be re-encrypted and then be accessible to the intended users; else none of the cipher texts can be re-encrypted or accessed by others.
- ❖ PGP and IBE, system is less efficient in the aspect of communication and not more practical in user experience.
- ❖ Users are not able to share the encrypted data to others lot of issue are occurring.
- ❖ No Identity provided for public keys to encrypt data.

OBJECTIVES OF THE THESIS

3.2 Proposed System:

- ❖ In this paper, we refine PRE by incorporating the advantages of IPRE, CPRE and BPRE for more flexible applications and propose a new concept of conditional identity based broadcast PRE (CIBPRE). In a CIBPRE system, a trusted key generation center (KGC) initializes the system parameters of CIBPRE, and generates private keys for users.
- ❖ To securely share files to multiple receivers, a sender can encrypt the files with the receivers' identities and file-sharing conditions. If later the sender would also like to share some files associated with the same condition with other receivers, the sender can delegate a re-encryption key labeled with the condition to the proxy, and the parameters to generate the re-encryption key is independent of the original receivers of these files. Then the proxy can re-encrypt the initial cipher texts matching the condition to the resulting receiver set.
- ❖ With CIBPRE, in addition to the initial authorized receivers who can access the file by decrypting the initial cipher text with their private keys, the newly authorized receivers can also access the file by decrypting the re-encrypted cipher text with their private keys.

Advantages of Proposed System:

- ❖ The sender does not need to download and re-encrypt repetitively, but delegates a single key matching condition to the proxy. These features make CIBPRE a versatile tool to secure remotely stored files, especially when there are different receivers to share the files as time passes.
- ❖ We define a practical security notion for CIBPRE systems. Intuitively, without the corresponding private keys, one can learn nothing about the plaintext hidden in the initial or re-encrypted CIBPRE cipher text; an initial cipher text cannot be correctly re-encrypted by a re-encryption key if the cipher text and the key are associated with different conditions.
- ❖ We propose an efficient CIBPRE that is provably secure in the above adversary model. We prove that the IND-SIDCPA security of the proposed CIBPRE scheme if the underlying identity-based broadcast encryption (IBBE) scheme is secure and the Decisional Bilinear Diffie-Hellman (DBDH) assumption holds. Our proposed CIBPRE scheme enjoys constant-size initial and re-encrypted cipher texts, and eliminates the constraints of the recent work

IV.MODULES:

- ❖ System Construction Module
- ❖ Proxy Re-encryption Module
- ❖ Trusted Key Generation Center (KGC)
- ❖ Cloud Email

4.1 System Construction Module:

- ❖ In this module a user can upload and send data to other users in cloud mail and other users can receive the data in cloud mail with a secure way. CIBPRE system, an trusted key generation center (KGC) initializes the system parameters of CIBPRE, and generates private keys for users.

- A sender can encrypt the files with the receivers' identities and file-sharing conditions. If later the sender would also like to share some files associated with the same condition with other receivers, the sender can delegate a re-encryption key labeled with the condition to the proxy, and the parameters to generate the re-encryption key is independent of the original receivers of these files. Then the proxy can re-encrypt the initial cipher texts matching the condition to the resulting receiver set. With CIBPRE, in addition to the initial authorized receivers who can access the file by decrypting the initial cipher text with their private keys, the newly authorized receivers can also access the file by decrypting the re-encrypted cipher text with their private keys. Note that the initial cipher texts may be stored remotely while keeping secret.
- The sender does not need to download and re-encrypt repetitively, but delegates a single key matching condition to the proxy.

4.2 Proxy Re-encryption Module:

- In Proxy re-encryption a User may encrypt his file with his own public key and then store the cipher text in an honest-but-curious server. When the receiver is decided, the sender can delegate a re-encryption key associated with the receiver to the server as a proxy.
- Then the proxy re-encrypts the initial cipher text to the intended receiver. Finally, the receiver can decrypt the resulting cipher text with her private key.
- The security of PRE usually assures that (1) neither the server/proxy nor non-intended receivers can learn any useful information about the (re-)encrypted file, and (2) before receiving the re-encryption key, the proxy cannot re-encrypt the initial cipher text in a meaningful way.

4.3 Trusted Key Generation Center (KGC):

- In this module Key generation is the process of generating keys in cryptography. A key is used to encrypt and decrypt whatever data is being encrypted/decrypted by user. The trusted key generation is used for initializes the system parameters of CIBPRE, and generates private keys for users.
- The KGC generates the system parameters to initialize the CIBPRE based cloud email system. It chooses a security parameter 2 N and a value N 2 N (the maximal number of receivers of an email), and runs algorithm Setup PRE to generate a pair of master public and secret keys PKPRE and MKPRE. It chooses a secure symmetric key encryption scheme.
- When a new user joins this system, the KGC generates a private key for him. Without loss of generality, let ID denote the email address of the new user. The KGC runs algorithm Extract to generate the private key SKPRE ID, and sends it to the user in a secure channel which is established by the SSL/TLS protocol.

4.4 Cloud Email:

- In this module CIBPRE-based cloud email system, the enterprise administrator only needs to initialize the system and generate the private key for the newly joined user. In other words, the enterprise administrator can be offline if no new user joins the system. It is a useful paradigm for the enterprise administrator to resist the outside attacks in practice.
- It is a useful paradigm for the enterprise administrator to resist the outside attacks in practice. The cloud server provides efficient services to send, store and forward users' encrypted emails. Moreover, it is convenient that all users take email addresses as public keys to encrypt emails. In the aspect of security, all users' emails are confidential even if the cloud sever is compromised.
- A user can send an encrypted email to other users. And this email will be stored in the cloud server. If the user wants to review this email, he can fetch the encrypted email from the cloud server and decrypt it. Suppose user ID1 wants to send the email content F (including the associated attachment) to the users.

4.5 SYSTEM REQUIREMENTS

4.5.1 HARDWARE REQUIREMENTS:

System	: Pentium IV 2.4 GHz.
Hard Disk	: 40 GB.
Floppy Drive	: 1.44 Mb.
Monitor	: 15 VGA Colour.
Mouse	: Logitech.
Ram	: 512 Mb.

4.5.2 SOFTWARE REQUIREMENTS:

Operating system	: - Windows XP/7.
Coding Language	: JAVA/J2EE
Data Base	: MYSQL

V.SYSTEM DESIGN

5.1 SYSTEM ARCHITECTURE:

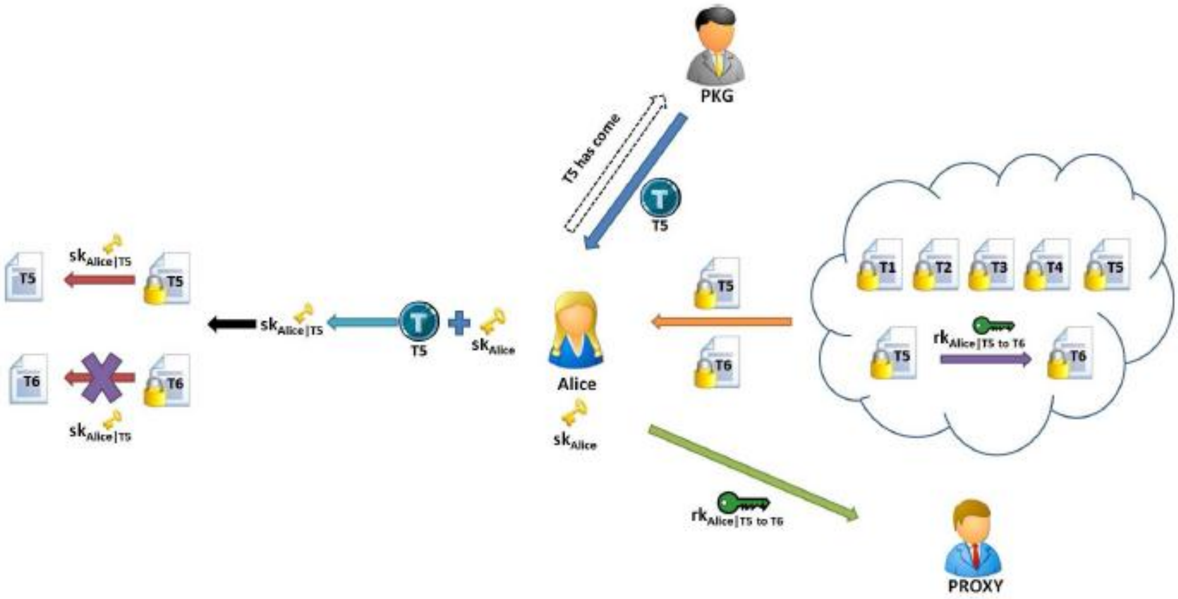

Fig: 5.1 System Architecture

VI.CONCLUSION

This paper presented a new kind of PRE concept called conditional identity-based broadcast proxy re-encryption (CIBPRE), as well as its IND-SID-CPA security definitions. The CIBPRE is a general concept equipped with the capabilities of conditional PRE, Identity-based PRE and broadcast PRE. The IND-SID-CPA security definition of CIBPRE incorporated the security requirements of CPRE, IPRE and BPRE. CIBPRE inherits the advantages of CPRE, IPRE and BPRE for applications. It allows a user to share their outsourced encrypted data with others in a fine-grained manner. All CIBPRE users takes their identities as public keys to encrypt data. It avoids a user to fetch and verify other users' certificates before encrypting his data. Moreover, it allows a user to generate a broadcast cipher text for multiple receivers and share his outsourced encrypted data to multiple receivers in a batch manner. We instantiated the first CIBPRE scheme based on the Identity-based broadcast encryption in [30]. Upon the provable security of the IBBE scheme and the DBDH assumption, the instance of CIBPRE is provably IND-Sidcpa secure in the RO model. It indicates that without the corresponding private key or the right to share a user's outsourced data, one can learn nothing about the user's data. Finally, we compared the proposed CIBPRE scheme with similar works and the comparison confirms the advantages of our CIBPRE scheme. We built the encrypted cloud email system based our CIBPRE scheme. Compared with the previous techniques such as PGP and IBE, our CIBPRE-based system is much more efficient in the aspect of communication and more practical in user experience.

REFERENCES

[1] M. Blaze, G. Bleumer, and M. Strauss, "Divertible protocols and atomic proxy cryptography," in Proc. Int. Conf. Theory Appl. Cryptographic Techn.: Adv. Cryptol., 1998, pp. 127–144.

[2] 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, pp. 458–475.

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

[4] T. Matsuo, "Proxy re-encryption systems for identity-based encryption," in Proc. 1st Int. Conf. Pairing-Based Cryptography, 2007, pp. 247–267.

[5] C.-K. Chu and W.-G. Tzeng, "Identity-based proxy re-encryption without random oracles," in Proc. 10th Int. Conf. Inf. Security, 2007, pp. 189–202.

[6] L. Ibraimi, Q. Tang, P. Hartel, and W. Jonker, "A type-and-identity- based proxy re-encryption scheme and its application in healthcare," in Proc.

5th VLDB Conf. Secure Data Manage., 2008, pp. 185–198.

[7] J. Shao, G. Wei, Y. Ling, and M. Xie, "Identity-based conditional proxy re-encryption," in Proc. IEEE Int. Conf. Commun., 2011, pp. 1–5.

[8] K. Liang, Z. Liu, X. Tan, D. S. Wong, and C. Tang, "A CCA-secure identity-based conditional proxy re-encryption without random oracles," in Proc. 15th Int. Conf. Inf. Security Cryptol., 2012, pp. 231–146.

[9] 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.

[10] Q. Tang, "Type-based proxy re-encryption and its construction," in Proc. 9th Int. Conf. Cryptol. India: Progress Cryptol. 2008, pp. 130–144.

[11] J. Weng, R. H. Deng, X. Ding, C.-K. Chu, and J. Lai, "Conditional proxy re-encryption secure against chosen-cipher text attack," in Proc. 4th Int. Symp. Inf., Comput. Commun.Security, 2009, pp. 322–332.

[12] J. Weng, Y. Yang, Q. Tang, R. H. Deng, and F. Bao, "Efficient conditional proxy re-encryption with chosen-cipher text security," in Proc. 12th Int. Conf. Inf. Security, 2009, pp. 151–166.

[13] L. Fang, W. Susilo, and J. Wang, "Anonymous conditional proxy re-encryption without random oracle," in Proc. 3rd Int. Conf. Provable Security, 2009, pp. 47–60.

[14] K. Liang, Q. Huang, R. Schlegel, D. S. Wong, and C. Tang, "A conditional proxy broadcast re-encryption scheme supporting timedrelease," in Proc. 9th Int. Conf. Inf. Security Practice Experience, 2013, pp. 132–146.