International Journal for Innovative
Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

COPY RIGHT

IJIEMR Transactions, online available on 24th February 2018. Link :
http://www.ijiemr.org/downloads.php?vol=Volume-7&issue=ISSUE-2

Title: An Efficient Encrypted Cloud Email System based CIBPRE Scheme for Store and Share data in Cloud.

Volume 07, Issue 02, Page No: 671 – 676.

Paper Authors

*** JALLEDA HYMAVATHI, G. CH. SRINIAVASA RAO.**

* Dept of CSE, Newton's Institute of Engineering.

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

AN EFFICIENT ENCRYPTED CLOUD EMAIL SYSTEM BASED CIBPRE SCHEME FOR STORE AND SHARE DATA IN CLOUD

*JALLEDA HYMAVATHI, **G. CH. SRINIAVASA RAO
*PG Scholar, Department of CSE, Newton's Institute of Engineering, Alugurajupalli Village, Macherla Mandal, Guntur, Andhra Pradesh, India
**Associate Professor, Department of CSE, Newton's Institute of Engineering, Alugurajupalli Village, Macherla Mandal, Guntur, Andhra Pradesh, India

ABSTRACT—

An expert and lingering report of Proxy Re-Encryption (PRE) together with indecisive proxy re-encryption (CPRE), Identity-based faultlessly alternate re-encryption and convey PRE (BPRE) have been predictable. An powerful and extended rendition of Proxy Re-Encryption (PRE, as an example, restrictive middleman re-encryption (CPRE), Identity-based intermediary re-encryption and talk PRE (BPRE) were proposed. This paper proposes a plan referred to as restrictive character primarily based communicate middleman re-encryption and gives a proficient safety to the capacity and recuperation of the information in disbursed garage. This plan permits a sender to encode the statistics and a sender can appoint a re-encryption key to an intermediary so starting discern content may be modified over to another one. On spotting the expected collector, middleman appoints the re-encoded key to the beneficiary utilizing which the facts is decoded. A productive CIBPRE plot with provable security has been proposed on this paper.

1. INTRODUCTION

Proxy re-encryption (PRE) gives a comfortable and flexible method for a sender to store and proportion statistics. A user may also encrypt his report with his very own public key after which save the ciphertext in an honest-however-curious server. When the receiver is determined, the sender can delegate a re-encryption key associated with the receiver to the server as a proxy. When the receiver is determined, the sender can delegate a re-encryption key associated with the receiver to the server as a proxy. Then the proxy re-encrypts the introductory ciphertext to the anticipated receiver. at long last, the recipient can decrypt the consequent ciphertext with her non-public key. The security of PRE typically assures that (1) neither the server/proxy nor non-intended receivers can analyze any beneficial records about the (re-)encrypted file. (2) Prior to unloading the re-encryption key, the proxy can't re-encrypt the preliminary ciphertext in a considerable way. Efforts had been through to supply PRE with quick-witted capabilities. The early PRE was proposed in the traditional public-key infrastructure placing which incurs complex certificates management. To relieve this trouble, several identity-primarily based PRE (IPRE) schemes were proposed so that the receivers' recognizable identities can function public keys. In its place of fetching and verifying the receivers' documentation, the sender and the proxy minimally want to distinguish the receivers' identities that are extra versatile in implement. PRE and IPRE permit a single receiver. If there are more receivers, the device desires to invoke PRE or IPRE a couple of times. To deal with this difficulty, the idea of broadcast PRE (BPRE) has been proposed. BPRE works in a comparable way as PRE and IPRE, however, greater flexibility. In the evaluation, BPRE allows a sender to generate an initial ciphertext to a receiver set, in preference to a single receiver. Further, the sender can delegate a re-encryption key associated with any other receiver set in order that the proxy can re-encrypt to. The above PRE schemes most effective permit the re-encryption technique is accomplished in an all-or-nothing way. The proxy can either re-encrypt all of the preliminary ciphertexts or none of them. This coarse-received manage over ciphertexts to be re-encrypted may also restrict the software of PRE systems. To fill this hole, a polished idea referred to as conditional PRE (CPRE) has been proposed. In CPRE schemes a sender can put into effect nice-grained re-encryption control over his initial ciphertexts. The sender achieves this intention by associating a condition with an encryption key. Only the ciphertexts assembly the required condition can be re-encrypted via the proxy maintaining the corresponding re-encryption key.

2. RELATED WORK

T. Matsuo proposed two proxy re-encryption structures; one for the decryption proper delegation from a CBE person to IBE users, and the other one for the delegation among IBE users. The former is the first "hybrid" proxy re-encryption device, and the latter has a few gain over the previously proposed identification based totally structures. He brought the security notion and proved that each our systems are semantically at ease primarily based at the dBDH assumption, in the fashionable model. Author offered neither a hybrid machine nor an identification-primarily based system at ease in the CCA feel.

C.-K. Chu and W. G. Tzeng brought new buildings permitting non-interactive, unidirectional proxy re-encryption in the IBE putting. Their schemes are very efficient and may be deployed inside preferred IBE frameworks. New compelling applications can be realized way to their schemes, maximum drastically characteristic-based delegation and get entry to control.

L. Ibraimi, Q. Tang, P. Hartel, and W. Jonker endorse a type-and-identification-primarily based proxy re-encryption scheme based on the Boneh-Franklin scheme which has been proved semantically comfy towards a chosen plaintext attack. Their scheme allows the delegator to offer distinctive re-encryption skills to the proxy even as using the same key pair. This asset is confirmed to be beneficial of their PHR disclosure scheme, where an character can easily implement satisfactory-grained get admission to manipulate regulations to his PHR data.

J. Weng, Y. Yang, Q. Tang, R. H. Deng, and F. Bao proposed a more green CCA secure unidirectional C-PRE scheme with much less variety of bilinear pairings. The scheme is greater stylish whilst in comparison to its opposite numbers. They have proved the safety of the scheme inside the random oracle version under appropriate protection definitions. There are nevertheless many open issues to be solved, which includes designing CCA relaxed CPRE scheme in the popular version, C-PRE in different settings like identity primarily based and certificateless cryptography.

M. Blaze, G. Bleumer, and M. Strauss introduce the belief of divertibility as protocol belongings instead of the existing notion as a language property. Other crucial examples falling beneath the new definition are blind signature protocols. They propose a sufficiency criterion for divertibility that is glad with the aid of many existing protocols and which, exceedingly, generalizes to cover numerous protocols no longer generally associated with divertibility (e.g., Diffie-Hellman key alternate). Next, they added atomic proxy cryptography, wherein an atomic proxy characteristic, in conjunction with a public proxy key, converts ciphertexts (messages or signatures) for one key into ciphertexts for every other. Proxy keys, as soon as generated, can be made public and proxy functions applied in untrusted environments. They presented atomic proxy functions for discrete-log-based encryption, identification, and signature schemes. It isn't always clean whether atomic proxy functions exist in preferred for all public-key cryptosystems.

3. FRAMEWORK

A. System overview

In this paper, we refine PRE with the aid of incorporating the blessings of IPRE, CPRE and BPRE for extra bendy programs and recommend a brand new concept of conditional identification based broadcast PRE (CIBPRE).Too securely percentage documents to more than one receiver, a sender can encrypt the files with the receivers' identities and file-sharing situations. If later the sender could also want to percentage some files related to the same circumstance with different receivers, the sender can delegate a re-encryption key labeled with the condition to the proxy, and the parameters to generate the re-encryption secret is unbiased of the unique receivers of those files. Then the proxy can re-encrypt the preliminary ciphertexts matching the situation to the ensuing receiver set. With CIBPRE, in addition to the initial legal receivers who can get entry to the record by means of decrypting the preliminary ciphertext with their private keys, the newly legal receivers also can access the file by using decrypting the re-encrypted ciphertext with their private keys. Note that the initial ciphertexts can be saved remotely at the same time as keeping secret. The sender does not want to down load and re-encrypt repetitively, but delegates a single key matching situation to the proxy. These functions make CIBPRE a versatile tool to cozy remotely stored documents, mainly whilst there are special receivers to share the documents as time passes.

B. Key Management

In this segment, while a new person joins this machine, the KGC generates a personal key for him. Without lack of generality, allow ID denotes the e-mail cope with of the new consumer. To generate the Non-public key and sends it to the consumer in a cozy channel that is mounted with the aid of the SSL/TLS protocol.

C. Send an Encrypted Cloud Email

In this phase, 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.

D. Work flow of Proposed CIBPRE

A consumer can ship an encrypted e-mail to other customers. And this electronic mail can be stored within the cloud server. If the consumer desires to assessment this email, he can fetch the encrypted e-mail from the cloud server and decrypt it. Suppose person ID1 wants to ship the email content material F (together with the associated attachment) to the users.

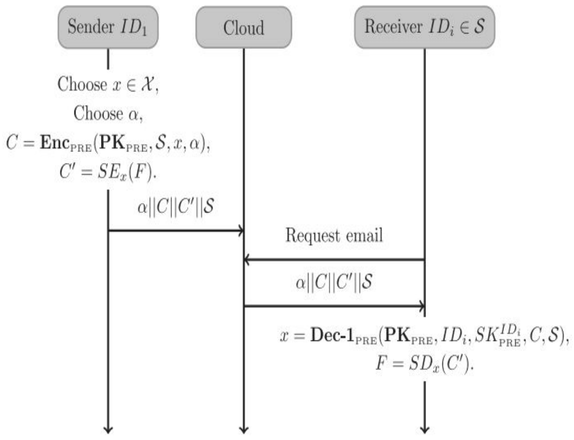

Sender ID_1
Cloud
Receiver $ID_i \in \mathcal{S}$
Choose $x \in \mathcal{X}$,
Choose α,
$C = \mathbf{Enc}_{\mathrm{PRE}}(\mathbf{PK}_{\mathrm{PRE}}, \mathcal{S}, x, \alpha)$,
$C' = SE_x(F)$.
$\alpha||C||C'||\mathcal{S}$
Request email
$\alpha||C||C'||\mathcal{S}$
$x = \mathbf{Dec\text{-}1}_{\mathrm{PRE}}(\mathbf{PK}_{\mathrm{PRE}}, ID_i, SK_{\mathrm{PRE}}^{ID_i}, C, \mathcal{S})$,
$F = SD_x(C')$.

Fig1. Sending Email

A consumer can ahead a records encrypted e mail to new customers by means of generating a re-encryption key for those customers and the challenge of this email.

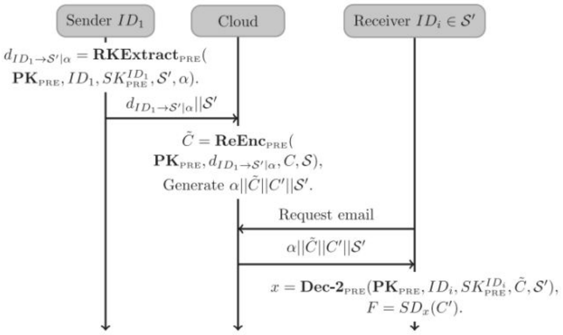
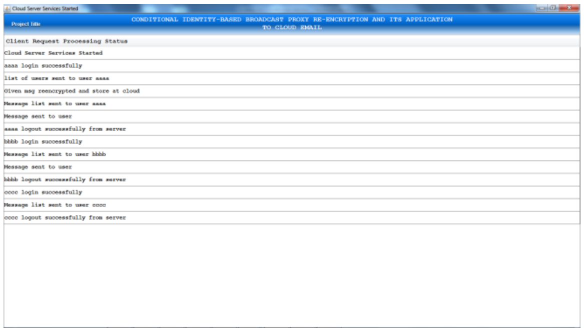

Sender ID_1
Cloud
Receiver $ID_i \in \mathcal{S}'$
$d_{ID_1 \to \mathcal{S}'|\alpha} = \mathbf{RKExtract}_{\mathrm{PRE}}($
$\mathbf{PK}_{\mathrm{PRE}}, ID_1, SK_{\mathrm{PRE}}^{ID_1}, \mathcal{S}', \alpha)$.
$d_{ID_1 \to \mathcal{S}'|\alpha}||\mathcal{S}'$
$\tilde{C} = \mathbf{ReEnc}_{\mathrm{PRE}}($
$\mathbf{PK}_{\mathrm{PRE}}, d_{ID_1 \to \mathcal{S}'|\alpha}, C, \mathcal{S})$,
Generate $\alpha||\tilde{C}||C'||\mathcal{S}'$.
Request email
$\alpha||\tilde{C}||C'||\mathcal{S}'$
$x = \mathbf{Dec\text{-}2}_{\mathrm{PRE}}(\mathbf{PK}_{\mathrm{PRE}}, ID_i, SK_{\mathrm{PRE}}^{ID_i}, \tilde{C}, \mathcal{S}')$,
$F = SD_x(C')$.

Fig2. Forward Email

Suppose user ID1 needs to forward his history encrypted email to the new users.

4. EXPERIMENTAL RESULTS

In this experiment, we need run the cloud server and proxy server. After run these two servers, we have to run the user application and users can register as well login into the system.

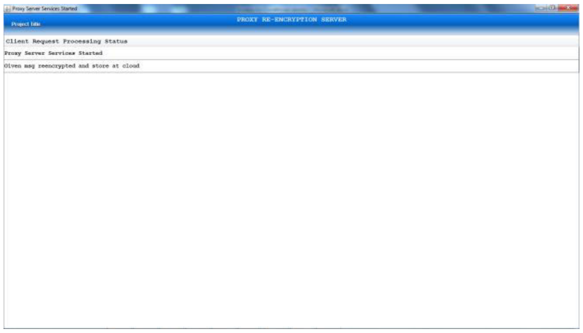

Cloud Server Services Started
Project Title
CONDITIONAL IDENTITY-BASED BROADCAST PROXY RE-ENCRYPTION AND ITS APPLICATION TO CLOUD EMAIL

```
Client Request Processing Status
Cloud Server Services Started
aaaa login successfully
list of users sent to user aaaa
Given msg reencrypted and store at cloud
Message list sent to user aaaa
Message sent to user
aaaa logout successfully from server
bbbb login successfully
Message list sent to user bbbb
Message sent to user
bbbb logout successfully from server
cccc login successfully
Message list sent to user cccc
cccc logout successfully from server
```

After login into the user application, he can compose the mail. At client side we are encrypting the message with AES algorithm and at proxy server side we are encrypting using Pairing based algorithm (JPair).

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

And the user's data will be stored at cloud server. The proxy server can re-encrypt the data at cloud.



```
Client Request Processing Status
Proxy Server Services Started
Given msg reencrypted and store at cloud
```

User can view his data and based on access control he can access the data.

5. CONCLUSION

In this paper we presented a brand new sort of PRE idea called conditional identification-based totally broadcast proxy re-encryption (CIBPRE), as well as its IND-sID-CPA safety definitions. The CIBPRE is a fashionable idea geared up with the competencies of conditional PRE, Identity-primarily based PRE and broadcast PRE. The IND-sID-CPA security definition of CIBPRE incorported the security necessities of CPRE, IPRE and BPRE; CIBPRE inherits the blessings of CPRE, IPRE and BPRE for applications. It permits a consumer to share their outsourced encrypted statistics with others in a best-grained way. All CIBPRE users take their identities as public keys to encrypt records. It avoids a user to fetch and verify different users' certificates before encrypting his statistics. Moreover, it allows a consumer to generate a printed ciphertext for multiple receivers and proportion his outsourced encrypted information to a couple of receivers in a batch manner.

REFERENCES

[1] M. Blaze, G. Bleumer, and M. Strauss, "Divertible protocols and atomic proxy cryptography," in Proc. Int. Conf. Theory Appl. Crytographic 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-ciphertext 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-ciphertext 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.