ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 6, June 2017

Conditional Identity Based Broadcast Proxy Re-Encryption with Self-Destruction in Cloud Email

Rajitha Radhakrishnan[1], Riyamol Sidhic[2]

P.G. Student, Department of Computer Science Engineering, Indira Gandhi Institute of Engineering and Technology for Women, Nellikuzhy, Kerala, India[1]

Associate Professor, Department of Computer Science Engineering, Indira Gandhi Institute of Engineering and Technology for Women, Nellikuzhy, Kerala, India[2]

ABSTRACT: Recently, a number of extended Proxy Re-Encryptions (PRE), e.g. Conditional (CPRE), identity-based PRE (IPRE) and broadcast PRE (BPRE), have been proposed for flexible applications. By incorporating CPRE, IPRE and BPRE, this paper proposes a versatile primitive referred to as conditional identity-based broadcast PRE (CIBPRE) and formalizes its semantic security. CIBPRE allows a sender to encrypt a message to multiple receivers by specifying these receivers' identities, and the sender can delegate a re-encryption key to a proxy so that he can convert the initial ciphertext into a new one to a new set of intended receivers. Moreover, the re-encryption key can be associated with a condition such that only the matching ciphertexts can be re-encrypted, which allows the original sender to enforce access control over his remote ciphertexts in a fine-grained manner. We propose an efficient CIBPRE scheme with provable security. In the instantiated scheme, the initial ciphertext, the re-encrypted ciphertext and the re-encryption key are all in constant size, and the parameters to generate a re-encryption key are independent of the original receivers of any initial ciphertext. Finally, we show an application of our CIBPRE to secure cloud email system advantageous over existing secure email systems based on Pretty Good Privacy protocol or identity-based encryption.

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

I. INTRODUCTION

PROXY re-encryption (PRE) provides a secure and flexi-ble method for a sender to store and share data. A user may encrypt his file with his own public key and then store the ciphertext 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 ciphertext to the intended receiver. Finally, the receiver can decrypt the resulting ciphertext 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 can not re-encrypt the initial ciphertext in a meaningful way. Efforts have been made to equip PRE with versatile capa-bilities. The early PRE was proposed in the traditional pub-lic-key infrastructure setting which incurs complicated certificate management. To relieve from this problem, several identity-based PRE (IPRE) schemes were proposed so that the receivers' recognizable identities can serve as public keys. Instead of fetching and verifying the receivers' certificates, the sender and the proxy just need to know the receivers' identities, which is more convenient in practice.

PRE and IPRE allows 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 [9]. BPRE works in a similar way as PRE and IPRE but more versatile. In contrast, BPRE allows a sender to generate an initial ciphertext to a receiver set, instead of a single receiver. Further, the sender can dele-gate a re-encryption key associated with another receiver set so that the proxy can re-encrypt to.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 6, June 2017

The shared data in cloud servers, however, usually contains users' sensitive information (e.g., personal profile, financial data, health records, etc.) and needs to be well protected [2]. As the ownership of the data is separated from the administration of them [3], the cloud servers may migrate users' data to other cloud servers in outsourcing or share them in cloud searching [4]. Therefore, it becomes a big challenge to protect the privacy of those shared data in cloud, specially in cross-cloud and big data environment [5]. In order to meet this challenge, it is necessary to design a comprehensive solution to support user-defined authorization period and to provide fine-grained access control during this period. The shared data should be selfdestroyed after the user-defined expiration time.

One of the methods to alleviate the problems is to storedata as a common encrypted form. The disadvantage of encrypting data is that the user cannot share his/her encrypted data at a fine-grained level. When a data owner wants to share someone his/her information, the owner must know exactly the one he/she wants to share with [6]. In many applications, the data owner wants to share information with several users according to the security policy based on the users' credentials. Attribute-based encryption (ABE) has significant advantages based on the tradition public key encryption instead of one-to-one encryption because it achieves flexible one-to-many encryption [7]. ABE scheme provides a powerful method to achieve both data security and fine-grained access control. In the key-policy ABE (KP-ABE) scheme to be elaborated in this paper, the ciphertext is labeled with set of descriptive attributes. Only when the set of descriptive attributes satisfies the access structure in the key, the user can get the plaintext [8].

II. RELATED WORK

Several other optional properties have been achieved in recent PRE schemes. The PRE schemes in [13], [24], [25] are equipped with an extra property that the receiver of a ciphertext is anonymous. The schemes in [26], [27] achieve multi-use bidirectional re-encryption. A ciphertext can be re-encrypted multiple times. Moreover, a re-encryption key realizes the bidirectional share between two users. Specifi-cally, if Alice delegates a re-encryption key to a proxy for re-encrypting her ciphertexts to Bob. The re-encryption key can also enable to re-encrypt Bob's ciphertexts to Alice. These two PRE schemes are provably secure under the cho-sen-ciphertext attack respectively in the random oracle and standard models. In contrast, the PRE scheme in [21] is multi-use unidirectional PRE schemes in which bidirec-tional re-encryption is forbidden. The work in [28] defines a general notion for PRE, which is called deterministic finite automata-based functional PRE (DFA-based FPRE), and proposes a concrete DFA-based FPRE system. The recent work in [29] proposes cloud-based revocable identity-based proxy re-encryption that supports user revocation and dele-gation of decryption rights.

Attribute-Based Encryption

Attribute-based encryption is one of the important applicationsof fuzzy identity-based encryption [7]. ABE comes intwo flavors called KP-ABE [8], [11] and ciphertext-policyABE (CP-ABE) [12], [13]. In CP-ABE, the ciphertext is associatedwith the access structure while the private key containsa set of attributes. Bethencourt et al. proposed the first CPABEscheme [12], the drawback of their scheme is that securityproof was only constructed under the generic groupmodel.

Secure Self-Destruction Scheme

A well-known method for addressing this problem is securedeletion of sensitive data after expiration when the data was used [19]. Recently, Cachin et al. employed a policy graph todescribe the relationship between attributes and the protection class and proposed a policy-based secure datadeletion scheme [20]. Reardon et al. leveraged the graphtheory, B-tree structure and key wrapping and proposeda novel approach to the design and analysis of securedeletionor persistent storage devices [21]. Because ofthe properties of physical storage media, the above-mentioned methods are not suitable for the cloud computingenvironment as the deleted data can be recovered easilyin the cloud servers [22].

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 6, June 2017

Time-Specific Encryption

The time-specific encryption scheme TSE, proposed byPeterson and Quaglia [10], was introduced as an extensionof TRE [9]. In TRE, a piece of protected data can beencrypted in such a way that it cannot be decrypted (evenby a legitimate receiver who owns the decryption key forthe ciphertext) until the time (called the release-time) thatwas specified by the encryptor. Most of the previousTRE schemes that adopt a time-sever model are in factpublic-key TRE schemes. They do not consider the sensitivedata privacy after expiration [30], [31], [32].In the TSE scheme, a time sever broadcasts a time instantkey (TIK), a data owner encrypts a message into a ciphertextduring a time interval, and a receiver can decrypt theciphertext if the TIK is valid in that interval. Kasamatsuet al. designed an efficient TSE scheme by using forwardsecureencryption (FSE) in which the size of the ciphertext isgreatly small than that generated by the previous schemes[33]. The time interval may be considered as the authorizationperiod of the protected data, and TSE schemes are ableto meet this requirement. However, it is a tricky problemwhen the traditional TSE is used in the cloud computingenvironment: cloud computing environment needs a finegrainedaccess control [17], which cannot be provided bythe traditional TSE schemes. How to achieve the time-specifiedciphertext into a fine-grained access control level is aproblem to be explored.

III.LITERATURE SURVEY

1.CPRE SECURE AGAINST CHOSEN-CIPHERTEXT ATTACK

Proxy re-encryption has found many practical applications, such as encrypted email forwarding, secure distributed le systems, and outsourced ltering of encrypted spam. We use the encrypted email forwarding as an example to illustrate the usage of PRE and to motivate our work as well. Imagine that a department manager, Alice, is to take a vacation. She delegates her secretary Bob to process her routine emails. Among the incoming emails, some could be encrypted under Alice's public key. Traditional public key encryption schemes does not allow Bob to process such emails, following the security norm that one's private key should never be shared with other. With a PRE system, Alice can simply give the email server a re-encryption key. For an encrypted incoming email, the email server (i.e. the proxy in PRE's jargon) transforms it into an encryption for Bob. Then Bob can read this email using his secret key. When Alice is back, she instructs the email server to stop the transformation.

2.A DFA-Based Functional PRE

FUNCTIONAL Encryption (FE) is a useful cryptographic Fprimitive that not only guarantees the confidentiality of data but also enhances the flexibility of data sharing.It is a general extension of Public Key Encryption (PKE). In traditional PKE, a data is encrypted to a particular receiver whose public key has registered to a trusted Certificate Author-ity. FE, however, provides more flexibility that the data can be encrypted under a description a, and the encryption can be decrypted if and only if there is a secret key whose description b matches a. As stated in and, a classicexample of FE is Attribute-Based Encryption (ABE) which comes to two flavors: Key-Policy ABE (KPABE) and Ciphertext-Policy ABE (CPABE). The former associates a secret key with an access policy such that the key can decrypt a ciphertext associated with attributes satisfying the policy. The latter, however, is complementary.

3.IB-PRE Without Random Oracles

In an identity-based proxy re-encryption (IB-PRE)scheme, a semi -trusted proxy can convert a ciphertext under Alice’s identity into a ciphertext for Bob. The proxy does not know the secret key of Alice or Bob, and also does not know the plaintext during the conversion. However, some scenarios require handle a fine-grained delegation. In this paper, by using the identity-based encryption (IBE) technique of Boneh-Boyen, we propose a new identity- based conditional proxy re-encryption (IBCPRE) scheme, which enables Alice to implement fi ne-grained delegation of decryption rights, and thus is more useful in many applications. Our scheme has significant advantages in both computational and communicational than Shao et al.’s IBCPRE scheme

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 6, June 2017

4.C-PRE With Chosen-Ciphertext Security

In a proxy re-encryption (PRE) scheme a semi-trusted proxy can convert a ciphertext under Alice's public key into a ciphertext for Bob. The proxy does not know the secret key of Alice or Bob, and also does not know the plaintext during the conversion. Conditional proxy re-encryption (C-PRE) can implement fine-grained delegation of decryption rights, and thus is more useful in many applications. In this paper, we propose an efficient C-PRE scheme, and prove its chosen-ciphertext security under decisional bilinear Diffie-Hellman (DBDH) assumption in the random oracle model. Our scheme has significant advantages in both computational and communicational than previous schemes.

The proxy is able to re-encrypt all ciphertexts from the delegator to the delegatee during the traditional PRE scheme. As a result, it is difficult for the delegator to implement any further fine-grained delegation of decryption rights. Suppose the delegator Alice wants delegatee Bob only to decrypt part of her ciphertexts. In this case, the delegator can only trust the proxy to implement her policies by re-encrypting the legitimate ciphertexts. This approach is infeasible because of the high-trust requirements on the proxy (for example, the proxy can be corrupted or collude with a malicious delegatee).

5.IBE Without Random Oracles

Identity-Based Encryption (IBE) provides a public-key encryption mechanism where a public key is an arbitrary string such as an email address or a telephone number. The corresponding private key can only be generated by a Private-Key Generator (PKG) who has knowledge of a master secret. In an IBE system, users authenticate themselves to the PKG and obtain private keys corresponding to their identities. The identity-based encryption concept was first proposed two decades ago and several approaches were subsequently suggested in a few precursor papers. It is only a few years ago, however, that a formal security model and a practical implementation were proposed. Boneh and Franklin define a security model for identity-based en-cryption and give a construction based on the Bilinear Diffie–Hellman (BDH) problem. Cocks describes another construction using quadratic residues modulo a compos-ite (see also). Gentry et al. give a construction using lattices. The security of all these systems requires cryptographic hash functions that are modeled as random oracles; i.e., these systems are only proven secure (under non-interactive assumptions) in the random-oracle model . A natural question is to devise a secure IBE system without random oracles.

IV.CIBPRE

Referring to the concept of CIBPRE, roughly speaking, both the initial CIBPRE ciphertext and the re-encrypted CIBPRE ciphertext are the IBBE ciphertexts. But it is different with an IBBE scheme that CIBPRE provides algorithms to trans-form an IBBE ciphertext (corresponding to an initial CIBPRE ciphertext) into another IBBE ciphertext (corresponding to an re-encrypted CIBPRE ciphertext). Moreover, the trans-formation is correct if it satisfies the consistencies defined by CIBPRE. Therefore, in order to construct a CIBPRE scheme, we refers to the D07 scheme which was reviewed in Section 2. Compared with the D07 scheme, the pro-posed CIBPRE scheme associates a D07 IBBE ciphertext with a new part to generate an initial CIBPRE ciphertext.

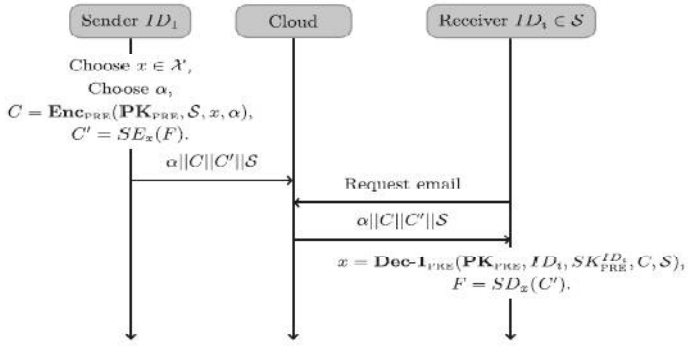
ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

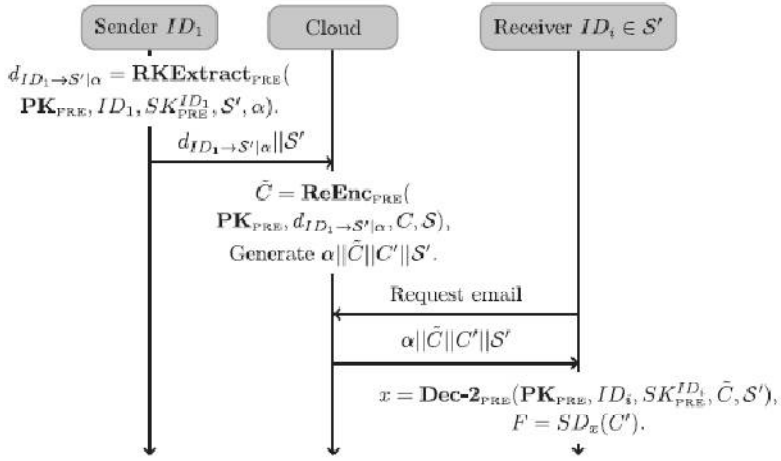
(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 6, June 2017



(a) Send an email.



(b) Forward an email.

- ID_1: an email sender;
- ID_i: an email receiver;
- $\mathcal{S}$: the identity set of the original receivers;
- $\mathcal{S}'$: the identity set of the new receivers;
- x: a symmetric key;
- α: the subject of an email;
- C: an initial CIBPRE ciphertext;
- C': a symmetric-key ciphertext;
- $SK_{\mathrm{PRE}}^{ID_i}$: the private key of user ID_i;
- $\mathbf{PK}_{\mathrm{PRE}}$: the master public key of CIBPRE;
- F: the content of an email;
- $d_{ID_1 \to \mathcal{S}'|\alpha}$: a re-encryption key;
- $\tilde{C}$: a re-encrypted CIBPRE ciphertext;

(c) The related notions.

- Setup $_{Pre}$ (λ, N) :given a security parameter λ€N, and the value N (maximum Number of receivers in each encryption),this algorithm possibilitically constructs bilinear map ê : G x G⟶ G_T where G and G_T are two multiplicative group with prime order *p*and |*p*|= λ, randomly chooses (*g*,*h*,*u*,*t*) € G^4 and γ = $Z^*_{p,}$ choses two cryptographic hash functions H : $\{0,1\}^* \longrightarrow Z^*_p$And H' : $G_T \longrightarrow$ G, finally outputs a master public key

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 6, June 2017

PK_{PRE}= $(p,G,G_T ,\hat{e}, w, v, h,h^{\gamma},\ldots\ldots\ldots\ldots h^{\gamma n}, u, u^{\gamma},\ldots\ldots\ldots\ldots u^{\gamma N}, t, t^{\gamma},\ldots\ldots\ldots\ldots\ldots t^{\gamma N}, H, H')$ and the master secret key $MK_{PRE} = (g,\gamma)$, where $w= g^{\gamma}$ and $v= \hat{e}(g,h)$

- $Extract_{PRE}$ ($MK_{PRE,}$ *ID*) : Given MK_{PRE} and identity *ID*, this algorithm outputs the privatr private keyPrivate key $SK^{ID}_{PRE} = g^{(1/\gamma+H(ID)).}$
- ENC_{PRE} : (PK_{PRE}, *S, m,* α). Given PK_{PRE} a set S of some identities (where $|S|\leq N$),
  A Plain text $m \in G_T$ and a condition $\alpha \in Z^*_p$. This algorith randomly picks
  $k \in Z^*_p$ and outputs an intial CIBPRE Ciphertext C= (c_1,c_2,c_3,c_4) where
  $c_1 = w^{-k}$
  $c_2 = h^{k\prod IDi\in S(\gamma+H(IDi))}$
  $c_3 = v^k.m$
  $c_4 = (u. t^{\alpha})^{k.\prod IDi \in S ((\gamma+H (IDi)) / H (IDi))}$
- **RKExtract**$_{PRE}$(**PK**$_{PRE}$, *ID*, SK^{ID}_{PRE}, *S', α*) : Given **PK**$_{PRE}$ an identity ID That is private keySK^{ID}_{PRE}, a set S' of some identities where S' $\leq N$ And a condition $\alpha \in Z^*_P$, this programme randomly picks $(k',s) \in Z^{*2}_p$ And outputs a re-encryption key $d_{ID \longrightarrow S'|\alpha} = (d_1, d_2, d_3, d_4)$ where

  $d_1 = w^{-k'}$
  $d_2= h^{k'\prod IDi\in S'(\gamma+H(IDi))}$
  $d_3 = H'' (v^{k'}). h^s$
  $d_4 = SK^{ID}_{PRE} . (u . t^{\alpha})^{s/(H(ID))}$
- $ReENE_{PRE}$ ($PK_{PRE,}$ $d_{ID \longrightarrow S'|\alpha}$,C, S) : Given PK_{PRE}, a re-encryption Key $d_{ID \longrightarrow S'|\alpha}$, $= (d_1, d_2, d_3, d_4)$,an initial CIBPRE Cibhertext C= (c_1, c_2, c_3, c_4), and a set *S* of some identities (where $|S|\leq N$), This Algorithm outputs a re-encrypted CIBPRE Cibhertext $\hat{C} = (\hat{c}_1, \hat{c}_2, \hat{c}_3, \hat{c}_4, \hat{c}_5)$
  Where $\hat{c}_1 = d_1 \hat{c}_2 = d_2 \hat{c}_3 = d_3 \hat{c}_4 = c_4$
  $\hat{c}_5 = c_3 . (\hat{e}(c_1,h^{\Delta\gamma (ID,S)}). \hat{e}(d_4, c_2))^{(-1/(\prod IDi\in S\Lambda IDi\neq ID\, HIdi)))}$
  with $\Delta\gamma (ID,S) = \gamma^{-1}. (IDi \in S\Lambda^{\prod} IDi\neq ID^{(\gamma+(H(IDi))}) - (IDi \in S\Lambda^{\prod} IDi\neq ID^{((H(IDi)}$
- Dec^{-1}_{PRE} (PK_{PRE} ,*ID*, $SK^{ID}_{PRE,}$ *C, S*) : Given PK_{PRE} an identity *ID* and its private key SK^{ID}_{PRE}. ,an initial CIBPRE CibhertextC= (c_1,c_2,c_3,c_4) and set S of some identities (where $|S|\leq N$), this algorithm computes

  $K = (\hat{e}(c_1,h^{\Delta\gamma(ID,S)}. \hat{e}(SK^{ID}_{PRE},c_2)^{(1/(\prod IDi\in S\Lambda IDi\neq ID\, HIdi))}$
  With $\Delta\gamma (ID,S) = \gamma^{-1}. (IDi \in S\Lambda^{\prod} IDi\neq ID^{(\gamma+(H(IDi))}) - (IDi \in S\Lambda^{\prod} IDi\neq ID^{((H(IDi)}$
  And finally outputs a plaintext m=c_3/K.
- Dec^{-2}_{PRE} (PK_{PRE} ,*ID*, $SK^{ID'}_{PRE,}$ $\hat{C}$, *S'*) : Given PK_{PRE} an identity *ID'* and its private key $SK^{ID'}_{PRE}$. ,an initial CIBPRE Cibhertext $\hat{C} = (\hat{c}_1, \hat{c}_2, \hat{c}_3, \hat{c}_4, \hat{c}_5)$and set *S'* of some identities (where $|S'|\leq N$), this algorithm computes

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 6, June 2017

$$K = (\hat{e}(\hat{c}_1, h^{\Delta\gamma(ID',S')}.\hat{e}(SK^{ID'}{}_{PRE}, \hat{c}_2)^{(1/(\prod IDi \in S' \wedge IDi \neq ID\ HIdi))}$$

With $\Delta\gamma\ (ID',S') = \gamma^{-1}.\ (IDi \in S' \wedge \prod IDi \neq ID^{(\gamma+(H(IDi))}) - (IDi \in S' \wedge \prod IDi \neq ID^{((H(IDi'))})$

Computes K' = $\hat{c}_3$/ (H'(K)' and finally outputs a plaintext m=$\hat{c}_5$.ê (K',$\hat{c}_4$)

V. RESULTS &CONCLUSION

CIBPRE inherits the advantages of CPRE, IPRE and BPRE for applications. It allows a user to share their out-sourced 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 ciphertext for multiple receivers and share his outsourced encrypted data to multi-ple receivers in a batch manner.With the rapid development of versatile cloud services, a lotof new challenges have emerged. One of the most importantproblems is how to securely delete the outsourced datastored in the cloud severs.

TABLE 5
Time Cost of Algorithms Enc_{PRE}, $Dec\text{-}1_{PRE}$, $RKExtract_{PRE}$, $ReEnc_{PRE}$ and $Dec\text{-}2_{PRE}$

Number of Receivers	Time Cost (Unit: CPU cycle)				
	Enc_{PRE}	$Dec\text{-}1_{PRE}$	$RKExtract_{PRE}$	$ReEnc_{PRE}$	$Dec\text{-}2_{PRE}$
4	34397064 (13.230 ms)	79089153 (30.419 ms)	36721919 (14.124ms)	78398268 (30.153 ms)	123970236 (47.681 ms)
8	54009982 (20.773 ms)	88327408 (33.972 ms)	41353858 (15.905 ms)	86587345 (33.303 ms)	128471538 (49.412 ms)
12	74940619 (28.823 ms)	96779670 (37.223 ms)	49816676 (19.160 ms)	93755987 (36.060 ms)	136606496 (52.541 ms)

In this paper, we proposed anovel KP-TSABE scheme which is able to achieve the timespecifiedciphertext in order to solve these problems byimplementing flexible fine-grained access control duringthe authorization period and time-controllable self-destructionafter expiration to the shared and outsourced data incloud computing. We also gave a system model and a securitymodel for the KP-TSABE scheme. Furthermore, weproved that KP-TSABE is secure under the standard modelwith the decision l-Expanded BDHI assumption. The comprehensiveanalysis indicates that the proposed KP-TSABEscheme is superior to other existing schemes.

Computational Cost

	KP-TSABE
Setup	2ω
Encryption	$1\psi + 1\omega + 1\varpi + \lvert S_{att}\rvert(m_{R,i} + 3 + c_{L,i})\omega$
Key generation	$\lvert S_Y\rvert(2\lvert T\rvert + 6)\omega$
Decryption	$O(TREE)\varpi + \lvert\vartheta\rvert[4\psi + (4T + 11 - n_x - c_x)\omega]$

Communication Overhead

Communication overhead	KP-TSABE
Data owner to cloud server	$1\lvert\mathbb{G}'\rvert + (1 + 2\lvert S_{att}\rvert)\lvert\mathbb{G}\rvert$
Authority to user	$\lvert S_Y\rvert(2\lvert T\rvert + 3 - n_x - m_x)\lvert\mathbb{G}\rvert$

REFERENCES

[1] M. Blaze, G. Bleumer, and M. Strauss, "Divertible protocols and atomic proxy cryptography," in Proc. Int. Conf. Theory Appl. Cryto-graphic Techn.: Adv. Cryptol, pp. 127–144., 1998.
[2] T. Matsuo, "Proxy re-encryption systems for identity-based encryption," in Proc. 1st Int. Conf. Pairing-Based Cryptography, pp. 247–267, 2007
[3] L. Ibraimi, Q. Tang, P. Hartel, and W. Jonker, "A type-and-iden-tity-based proxy re-encryption scheme and its application in healthcare," in Proc. 5th VLDB Conf. Secure Data Manage.,, pp. 185–198 ,2008.
[4] D. Boneh and X. Boyen, "Secure identity based encryption with-out random oracles," in Proc. 24th Annu. Int. Cryptol. Conf.: Adv. Cryptol., pp. 197–206,2004.
[5] R. Canetti and S. Hohenberger, "Efficient Selective Identity-Based Encryption Without Random Oracles" in Proc. 14th ACM Conf. Comput. Commun. Security, pp. 185–194,2007
[6] C.-K. Chu, J. Weng, S. S. M. Chow, J. Zhou, and R. H. Deng, "Efficient Conditional Proxy Re-Encryption With Chosen-Ciphertext Security" in Proc. 14th Aus-tralasian Conf. Inf. Security Privacy, pp. 327–342,2009.
[7] J. Shao, G. Wei, Y. Ling, and M. Xie, "A Dfa-Based Functional Proxy Re-Encryption Scheme For Secure Public Cloud Data Sharing" in Proc. IEEE Int. Conf. Commun., pp. 1–5,2011.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 6, June 2017

[8] C.-K. Chu and W.-G. Tzeng, "Identity-based proxy re-encryption without random oracles," in Proc. 10th Int. Conf. Inf. Security, 189–202, 2007.
[9] L. Ibraimi, Q. Tang, P. Hartel, and W. Jonker, "A type-and-iden-tity-based proxy re-encryption scheme and its application in healthcare," in Proc. 5th VLDB Conf. Secure Data Manage., pp. 185–198,2008.
[10] J. Shao, G. Wei, Y. Ling, and M. Xie, "A Secure Data Self-Destructing Scheme In Cloud Computing" in Proc. IEEE Int. Conf. Commun, pp. 1–5,2011.
[11] K. Liang, Z. Liu, X. Tan, D. S. Wong, and C. Tang, "A CCA-secureidentity-based conditional proxy re-encryption without random oracles," in Proc. 15th Int. Conf. Inf. Security Cryptol.,231–146,2012.
[12] 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,, pp. 322–332,2009.