International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue 14
November 2017

Cloud application with conditional identity based broadcast proxy re-encryption

K.Rajeshwari ; B.Krishna ; V.Janaki
1.PG Scholar, Department of CNIS,Vaagdevi College of Engineering, Bollikunta, Warangal, Telangana
Mail id:rajeshwari075@gmail.com
2.Asst. Professor Department of CSE, Vaagedevi College of Engineering, Bollikunta, Warangal, Telangana Mail id : bandikrishna007@gmail.com
3. Professor,HOD Depertment of CSE, Vaagedevi College of Engineering, Bollikunta, Warangal,Telangana

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.

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 capabilities. 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. 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 (KPABE) 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 are equipped with an extra property that the receiver of a ciphertext is anonymous. The schemes in 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 is multi-use unidirectional PRE schemes in which bidirectional re-encryption is forbidden. The work in 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 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 applications of fuzzy identity-based encryption . ABE comes into flavors called KP-ABE and ciphertext-policy ABE (CP-ABE) . In CP-ABE, the ciphertext is associated with the access structure while the private key contains set of attributes. Bettencourt et al. proposed the first CPABE scheme [12], the drawback of their scheme is that security proof was only constructed under the generic group model. Secure Self-Destruction Scheme A well-known method for addressing this problem is secure deletion of sensitive data after expiration when the data was used [19]. Recently, Caching et al. employed a policy graph to describe the relationship between attributes and the protection class and proposed a policy-based secure data deletion scheme [20]. Reardon et al. leveraged the graph theory, B-tree structure and key wrapping and proposed novel approach to the design and analysis of secure deletionor persistent storage devices [21]. Because of the

properties of physical storage media, the abovementioned methods are not suitable for the cloud computing environment as the deleted data can be recovered easily in the cloud servers [22] 0 Time-Specific Encryption The time-specific encryption scheme TSE, proposed by Peterson and Quigley [10], was introduced as an extension of TRE [9]. In TRE, a piece of protected data can be encrypted in such a way that it cannot be decrypted (even by a legitimate receiver who owns the decryption key forth ciphertext) until the time (called the release-time) that was specified by the encrypt or. Most of the previous TRE schemes that adopt a time-sever model are in fact publickey TRE schemes. They do not consider the sensitive data privacy after expiration In the TSE scheme, a time sever broadcasts a time instant key (TIK), a data owner encrypts a message into a cipher text during a time interval, and a receiver can decrypt the cipher text if the TIK is valid in that interval. Kasamatsuet al. designed an efficient TSE scheme by using forward secure encryption (FSE) in which the size of the ciphertext is greatly small than that generated by the previous schemes[33]. The time interval may be considered as the authorization period of the protected data, and TSE schemes are able to meet this requirement. However, it is a tricky problem when the traditional TSE is used in the cloud computing environment: cloud computing environment needs a finegrained access control [17], which cannot be provided byte traditional TSE schemes. How to achieve the time-specified ciphertext into a fine-grained access control level is a problem 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 classic example 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

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 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 0.15680/IJIRSET.2017.0606199 11190 Setup Pre (λ, N) :given a security parameter λ€N, and the value N (maximum Number of receivers 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 each encryption),this algorithm possibilitically constructs bilinear map ê : G x G GT where G and GT are two multiplicative group with prime order pand ׀p׀ =λ, randomly chooses (g,h,u,t) € G4 and γ = Z * p, choses two cryptographic hash functions H : {0,1}* Z * pAnd H' : GT 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 Copyright to IJIRSET DOI:10.15680/IJIRSET.2017.0606199 11191 PKPRE= (p,G,GT ,ê, w, v, h,hγ ,……h γn , u, u γ ,…….u γN, t, tγ ,…… tγN, H, H') and the master secret key MKPRE = (g,γ), where w= g γ and v= ê (g,h) ExtractPRE (MKPRE, ID) : Given MKPRE and identity ID, this algorithm outputs the privatr private keyPrivate• key SKID PRE = g (1/γ+H(ID)). ENCPRE : (PKPRE, S, m, α). Given PKPRE a set S of some identities (where ׀S׀≥N),• A Plain text m € GT and a condition α € Z* p. This algorith randomly picks k € Z* p and outputs an intial CIBPRE Ciphertext C= (c1,c2,c3,c4) where c1 = w -k c2 = h k∏ IDi€S(γ+H(IDi)) c3 = v k .m c4 = (u. t α) k.∏.IDi € S ((γ+H (IDi)) / H (IDi)) RKExtractPRE(PKPRE , ID, SKID• PRE, S', α) : Given PKPRE an identity ID That is private keySKID PRE, a set S' of some identities where S' ≤ ó And a condition α € Z* P, this programme randomly picks (k',s) € Z* p 2 And outputs a re-encryption key dID S'׀α = (d1, d2, d3, d4) where d1 = w -k' d2= h k'∏ IDi€S'(γ+H(IDi)) d3 = H'' (vk'). hs d4 = SKID PRE . (u . tα) s/(H(ID)) ReENEPRE (PKPRE, dID S'׀α ,C, S) : Given PKPRE, a re-encryption Key dID S'׀α , = (d1, d2, d3, d4) ,an initial CIBPRE Cibhertext C= (c1, c2, c3, c4), and a set S of some identities (where ׀S׀≥N), This Algorithm outputs a re-encrypted CIBPRE Cibhertext Ĉ = (ĉ1, ĉ2, ĉ3, ĉ4, ĉ5) Where ĉ1= d1 ĉ2 = d2 ĉ3 = d3 ĉ4 = c4 ĉ5 = c3 . (ê(c1,h Δγ (ID,S)). ê(d4, c2))(-1/(∏IDi€ sΛIDi≠ ID HIdi))) with Δγ (ID,S) = γ-1 . (IDi € SΛ∏ IDi≠ID(γ+(H(IDi))) - (IDi € SΛ∏ IDi≠ID((H(IDi)) Dec-1 PRE (PKPRE ,ID, SKID PRE, C, S) : Given PKPRE an identity ID and its private key SKID PRE. ,an initial CIBPRE CibhertextC= (c1,c2,c3,c4) and set S of some identities (where ׀S׀≥N), this algorithm computes K = (ê(c1,h Δγ(ID,S). ê(SKID PRE,c2) (1/(∏IDi€ sΛIDi≠ ID HIdi)) With Δγ (ID,S) = γ-1 . (IDi € SΛ∏ IDi≠ID(γ+(H(IDi))) - (IDi € SΛ∏ IDi≠ID((H(IDi)) And finally outputs a plaintext m=c3/K. Dec-2PRE (PKPRE

,ID, SKID' PRE, Ĉ, S') : Given PKPRE an identity ID' and its private key SKID' PRE. ,an initial CIBPRE Cibhertext Ĉ = (ĉ1, ĉ2, ĉ3, ĉ4, ĉ5)and set S' of some identities (where ıS'ı≥N), this algorithm K = (ê(ĉ1,h Δγ(ID',S').ê(SKID' PRE,ĉ2) (1/(∏IDi€ s'ΛIDi≠ ID HIdi)) With Δγ (ID',S') = γ-1 . (IDi € S'Λ∏ IDi≠ID(γ+(H(IDi))) - (IDi €S'Λ∏ IDi≠ID((H(IDi')) Computes K' = ĉ3/ (H'(K)' and finally outputs a plaintext m=ĉ5.ê (K',ĉ4)

V CONCLUSION

we instantiated the first CIBPRE scheme based on the Identity-Based Broadcast Encryption (IBBE) in [30]. Upon the provable security of the IBBE scheme and the DBDH assumption, the instance of CIBPRE is provably IND-sID-CPA 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", Proc. Advances in CryptologyEUROCRYPT ' 98, Springer, Heidelberg, 1998, pp. 127-144.

[2] A. Boldyreva, M. Fischlin, A. Palacio and B. Warinschi, "A Closer Look at PKI: Security and Efficiency", Proc. PKC 2007 Springer, Heidelberg, 2007, pp. 458-475.

[3] M. Green and G. Ateniese, "Identity-Based Proxy Re-Encryption", Proc. ACNS 2007, Springer, Heidelberg, 2007, pp. 288-306.

[4] T. Matsuo, "Proxy Re-encryption Systems for Identity-Based Encryption", Proc. PAIRING 2007, Springer, Heidelberg, 2007, pp. 247-267.

[5] C.-K. Chu and W.-G. Tzeng, "Identity-Based Proxy Re-encryption Without Random Oracles", Proc. ISC 2007, Springer, Heidelberg, 2007, pp. 189-202.

[6] L. Ibraimi, Q. Tang, P. Hartel and W. Jonker, "A Type-and-Identitybased Proxy Re-Encryption Scheme and its Application in Healthcare", Proc. SECURE DATA MANAGEMENT 2008, Springer, Heidelberg, 2008, pp. 185-198.

[7] J. Shao, G. Wei, Y. Ling and M. Xie, "Identity-based Conditional Proxy Re-encryption", Proc. IEEE International Conference on Communications (ICC), 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", Proc. ICISC, 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", Proc. INFORMATION SECURITY AND PRIVACY 2009, Springer, Heidelberg, 2009, pp. 327-342.

[10] Q. Tang, "Type-Based Proxy Re-encryption and Its Construction", proc. INDOCRYPT, 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", Proc. ASIACCS '09, ACM, 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", Proc. Information Security 2009, Springer-Verlag, 2009, pp. 151-166.

[13] L. Fang, W. Susilo and J. Wang, "Anonymous Conditional Proxy Re-encryption without Random Oracle", Proc. ProvSec 2009, Springer, Heidelberg, 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 Timed-Release", Proc. ISPEC 2013, LNCS 7863, Springer, Heidelberg, 2013, pp. 132-146.

[15] Philip R. Zimmermann, "PGP Source Code and Internals", MIT Press, ISBN 0-262-24039-4, 1995.

[16] D. Boneh and M. Franklin, "Identity-Based Encryption from the Weil Pairing", Proc. Advances in Cryptology-CRYPTO 2001, Springer, Heidelberg, 2001, pp. 213-239.

[17] Radicati Group, "Cloud Business Email Market, 2014-2018", http://www.radicati.com/wp/wpcontent/uploads/2014/10/Cloud-Business-Email-Market-2014-2018-Executive-Summary.pdf, 2014.

[18] Proofpoint Group, "Cloud-based Archiving vs. On-Premises Legacy Archiving", http://video.proofpoint.com/id/cloud-basedarchiving-vs.-on-premises-legacy-archiving-TCO-white-paper, 2012.

[19] G. Ateniese, K. Fu, M. Green and S. Hohenberger, "Improved Proxy Reencryption Schemes with Applications to Secure Distributed Storage", ACM Transactions on Information and System Security, 2006, pp. 1-30.

[20] R.H. Deng, J. Weng, S. Liu and K. Chen, "Chosen-ciphertext secure proxy re-encryption without pairings", Cryptology and Network Security, vol. 5339, 2008, pp. 1-17. 13 0018-9340 (c) 2015 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information. This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TC.2015.2417544, IEEE Transactions on Computers

[21] V. Kirtane and C.P. Rangan, "RSA-TBOS signcryption with proxy re-encryption", Proceedings of the 8th ACM workshop on Digital rights management (DRM '08), 2008, pp. 59-66.

[22] B. Libert and D. Vergnaud, "Unidirectional Chosen-Ciphertext Secure Proxy Re-Encryption", Proc. PKC 2008, Springer, Heidelberg, 2008, pp. 360-379.