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 2, February 2017

A Survey on CIBPRE -Cloud Email without Garbage Collection

Ann Mathew[1], Ashil M.K [2], Rajasree M [3], Sam Kurian Jacob [4], Annie Chacko [5]

B. Tech Student, Department of Computer Engineering, MBC Engineering College, Idukki, Kerala, India[1,2,3,4]

Assistant Professor, HOD, Department of Computer Engineering, MBC Engineering College, Idukki, Kerala, India [5]

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 cipher text 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 cipher texts can be re-encrypted, which allows the original sender to enforce access control over his remote cipher texts in a fine-grained manner. We propose an efficient CIBPRE scheme with provable security. In the instantiated scheme, the initial cipher text, the re-encrypted cipher text 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 cipher text. 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. In this we can give the admin an extra provision to approve and reject the users on time of registration. It will bring more security to the system.

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

I. INTRODUCTION

Intermediary re-encryption gives a protected and adaptable technique for a sender to store and share information. A client may encode his record with his own particular open key and after that store the figure message in a fair however inquisitive server. At the point when the collector is chosen, the sender can assign a re-encryption key related with the beneficiary to the server as an intermediary. At that point the intermediary re-encodes the underlying figure content to the proposed recipient. At last, the collector can unscramble the subsequent figure content with her private key. The security of PRE generally guarantees that neither the server/intermediary nor non-proposed recipients can take in any helpful data about the re-scrambled file and before getting the re-encryption key, the intermediary can't re-encode the underlying figure message seriously. Endeavours have been made to furnish PRE with adaptable capacities.

The early PRE was proposed in the conventional open key framework setting which brings about muddled testament administration. To calm from this issue, a few personality based PRE (IPRE) plans were proposed so that the collector's conspicuous characters can fill in as open keys. Rather than getting and confirming the beneficiaries' declarations, the sender and the intermediary simply need to know the recipients' personalities, which is more helpful by and by.

PRE and IPRE permit a solitary beneficiary. On the off chance that there are more beneficiaries, the framework needs to summon PRE or IPRE numerous times. To address this issue, the idea of communicate PRE (BPRE) has been proposed. BPRE works in a comparable path as PRE and IPRE yet more flexible. Interestingly, BPRE permits a sender to produce an underlying cipher text to a beneficiary set, rather than a solitary beneficiary. Promote, the sender can appoint a re-encryption key related with another collector set so that the intermediary can re-encode to. The above PRE

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 2, February 2017

conspires just permits the re-encryption system is executed in a win or bust way. The intermediary can either re-encode all the underlying cipher texts or none of them. This coarse-picked up control over cipher texts to be re-scrambled may confine the utilization of PRE frameworks. To fill this hole, a refined idea alluded to as contingent PRE (CPRE) has been proposed. In CPRE plans a sender can uphold fine-grained re-encryption control over his underlying cipher texts. The sender accomplishes this objective by partner a condition with a re-encryption key. Just the cipher texts meeting the predefined condition can be re-scrambled by the intermediary holding the comparing re-encryption key.

A current restrictive intermediary communicate re-encryption conspire permits the senders to control the opportunity to re-encrypt their underlying cipher texts. At the point when a sender produces a re-encryption key to re-scramble an underlying cipher text, the sender needs to take the first recipients' personalities of the underlying cipher text as info. By and by, it implies that the sender should locally recollect the collectors' personalities of all beginning cipher texts. This necessity makes this plan compelled for the memory-constrained or versatile senders and productive just for extraordinary applications

II. RELATED WORKS

1.Giuseppe Ateniese, Kevin Fu, Matthew Green, Susan Hohenberger "Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage ."[3] Proxy re-encryption allows a proxy to transform a cipher text computed under ones public key into one that can be opened by others secret key. The primary advantage of this is that they are unidirectional and do not require delegators to reveal all of their secret key to anyone or even interact with the delegate in order to allow a proxy to re-encrypt their cipher texts. It is secure. The limitation is that not allow further delegation, only useful when trust between sender and receiver is mutual.

2. Alexandra Boldyreva,Marc Fischlin, Adriana Palacio, Bogdan Warinschi "A Closer Look at PKI: Security and Efficiency."[1] In this a closer look at the security and efficiency of public-key encryption and signature schemes in public-key infrastructures. Provide constructions for encryption and signature schemes that provably satisfy strong security definitions and are more efficient and powerful than the corresponding traditional constructions that assume a digital certificate issued by the CA must be verified whenever a public key is used.The limitation is that it have no idea about the security even when a CA become compromised and the Security analyses that do not explicitly include the behaviour of the CA or the key-registration protocol have been previously pointed out in other contexts.

3.Varad Kirtane, C. Pandu Rangan "RSA-TBOS Signcryption with Proxy Re-encryption."[9] In this available in the literature concerning authenticity, unforgeability and non-repudiation and propose a signature non-repudiation model suitable for sign-cryption schemes with proxy re-encryption. Avoid the stealing of plain text by the proxy. Here not using bilinear maps, any deviation from the protocol can be easily detected and simple performance.The limitation is may fail if able to detect that the values return are different from the actual values.

4. Cheng-Kang Chu, Jian Weng,Sherman S.M. Chow, Jianying Zhou and Robert H. Deng " Conditional Proxy Broadcast Re-Encryption."[2] In this, we formalize this notion, propose a basic CPBRE scheme secure against chosen-plaintext attacks, and an extension that is secure against replayable chosen-cipher text attacks(RCCA) . RCCA is a weaker variant of chosen-cipher text attack (CCA) in which a harmless mauling of the challenge cipher text is tolerated. fine-grained delegation, less communication cost, proxy is too powerful. The limitation are cannot issue some conditions to the decryption oracle, complexity in getting certain services to work through the proxy.

5. J.Weng,R.H.Deng,X.Ding,C,K Chu and J. Lai "Conditional Proxy Re-encryption Secure Against Chosen-Cipher text Attack."[5] In this contain the extention of C-PRE scheme to obtain a conditional proxy re-encryption system with multiple conditions (MC-PRE) scheme with multiple conditions. This scheme is infact only supports AND gates on conditions. It remains as an interesting open problem how to construct CCA-secure C-PRE schemes with anonymous conditions or supporting more expressive predicates. Here the server have a fine-grained control over the delegation, server can flexibly assign the delegate. The limitations are MC-PRE scheme is in fact only supports AND gates on conditions and if proxy doesn't have both the keys it is still impossible for them to compromise the delegator's security.

6. Toshihide Matsuda, Ryo Nishimaki, and Keisuke Tanaka "CCA Proxy Re-Encryption without Bilinear Maps in the Standard Model."[8].In the standard model,a bidirectional and multi-hop PRE-CCA scheme without bilinear maps is

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 2, February 2017

generated. This scheme generates a signature of a part of a cipher text in the encryption scheme. The original scheme generates a signature of all the main parts of a cipher text in the encryption process. It is bidirectional such that re-encryption key is identical.The limitation is that they do not guarantee several properties of re-applicable LTDFs and does not have the key-private property.

III.WORKING

CIBPRE permits a sender to encode a message to numerous recipients by indicating the collectors' characters, and the sender can designate a re-encryption key to an intermediary so he can change over the underlying cipher text into another one to another arrangement of planned beneficiaries. Additionally, the re-encryption key can be related with a condition to such an extent that lone the coordinating cipher texts can be re-scrambled, which permits the first sender to implement get to control over his remote cipher texts in a fine-grained way. We propose an efficient CIBPRE plot with provable security. In the instantiated plot, the underlying cipher text, the re-scrambled cipher text and the re-encryption key are all in consistent size, and the parameters to create a re-encryption key are autonomous of the first collectors of any underlying cipher text. At long last, we demonstrate a utilization of our CIBPRE to secure cloud email framework worthwhile over existing secure email frameworks in light of Pretty Good Privacy convention or personality based encryption.

The paper have some modules such as Data Owner, Admin,Proxy,Data user1and finally data user2.The User Registration page in the Data Owner module use the identity such as user name and password for the registration .The current user will login to the User login page. The User then sends or mails the information or data to the receiver. Here starts the encryption of the data. This is done by using secret key. The plain text that is send by the user is converted into cipher text after the encryption. The cipher text is the given to the cloud storage for the storage purpose. The stored data is then downloaded by the receiver. This cipher text is decrypted by using another secret key and thus the receiver can get the data. After downloading this can be send to the proxy. This is done for re-encrypting the data the re-encrypted data can be share among multiple users. The downloaded cipher text is again decrypted to get plain text.

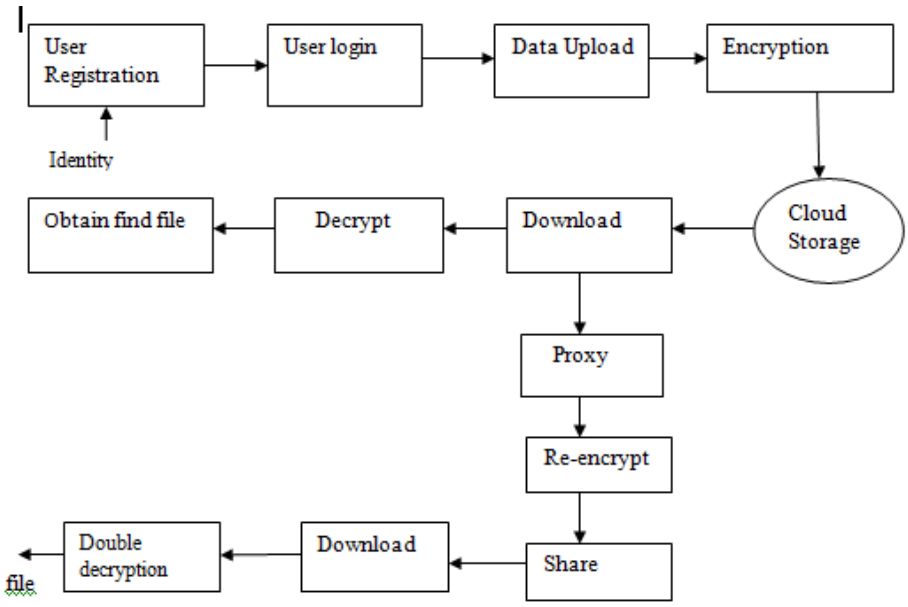

Fig: Working of CIBPRE

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 2, February 2017

The paper mainly focuses on the security of the encrypted data and eliminates the data being downloaded multiple times. The encryption, decryption and re-encryption is done by using some of the algorithms.

AES algorithm: AES (acronym of Advanced Encryption Standard) is a symmetric encryption algorithm. The algorithm was developed by two Belgian cryptographers Joan Daemen and Vincent Rijmen. AES was designed to be efficient in both hardware and software, and supports a block length of 128 bits and key lengths of 128, 192, and 256 bits.

Key generation algorithm is used for generating the secret keys like public key and the private key.And the next algorithm used is the conditional identity based algorithm for eliminating the garbage collection of the data.

IV.CONCLUSION

This paper shows PRE called CIBPRE and also with the security of information. It acquires the benefits of CPRE, IPRE and BPRE for applications. It permits a client to impart their outsourced scrambled information to others in a fine-grained way. All CIBPRE clients take their ways of life as open keys to encode information. It keeps away from a client to bring and confirm other clients' certificates before scrambling his information. In addition, it permits a client to produce a communicate cipher text for numerous beneficiaries and share his outsourced encoded information to various collectors in a bunch way. Cloud mailing with CIBPRE also reduces garbage collection.

REFERENCES

[1] A.Boldyreva,M.Fischlin,A.Palacio,and B.Warinschi,"A closer look at PKI Security and Efficiency",in Proc.10th Int .Conf. Theory Public-key Cryptography 2007.
[2] 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.
[3] G.Ateniese,K.Fu,M.Green,and S.Hohenberger,"Improved Proxy Re-encryption Schemes with Applications to Secure Distributed Storage",ACM Trans. Inf. Syst. Security, Vol. 9,2006
[4] J.Shao,G.Wei,Y.Ling,an M.Xie,"Identity Based Conditional Proxy Re-encryption", in Proc.IEE Int. Conf. Commun. ,2011
[5] J.Weng,R.H.Deng,X.Ding,C.K.Chu,and J.Lai,"Conditional Proxy Re-encryption Secure Against choosen Cipher text Attack",in Proc. 4th Int. Symp. Inf., Comput. Commun. Security,2009.
[6] K.Liang,M.H.Au,J.K.Liu,X.Qi,W.Susilo,X.P.Tran,D.S.Wong and G.Yang,"A DFA- Based Functional Proxy Re-encryption Scheme for Secure Public cloud data sharing",IEE Trans. Inf. Forensics Security,Vol.9,no.10,Oct-22014
[7] K.Liang,Q.Huang,R.Schlegel,D.S.Wong and C.Tang,"Conditional Proxy Broadcast Re-encryption Scheme Supporting TimedRelease",in Proc. 9th Int. Conf. Inf. Security Practice Excperience,2013
[8] T.Matsuda,R.Nishimaki and K.Tanaka,"CCA Proxy Re-encryption without bilinear maps in the standard model,"in Proc. 13t Int. Conf. Practice Theory Public key Cryptography,2010
[9] V.Kirtane and C.P.Rangan,"RSA-TBOS Signcryption with Proxy Re-encryption,"in Proc. 8th ACM Workshop Digital Rights Manage.,2008
[10] Peng Xu, Tengfei Jiao, Qianhong Wu, Wei Wang,and Hai Jin," Conditional Identity-Based Broadcast Proxy Re-Encryption and Its Application to Cloud Email"IEE Trans. On Computers, January 2016.