KGC Proxy Re-Encryption Scheme for Data Security in Cloud

R.Bhagya Sri

PG Student, Dept of CSE, G. Pulla Reddy Engineering College (Autonomous), Kurnool, AP-India

Bhagya.rayachuti123@gmail.com

G.Vijay Kumar

Associate Professor, Dept of CSE, G. Pulla Reddy Engineering College(Autonomous), Kurnool, AP-India

gvjykumar@gmail.com

ABSTRACT

Recently, number of proxy re-encryption schemes e.g. identity based, conditional based, broad cast proxy re-encryptions has been proposed for flexible applications. Proxy Re-Encryption permits a sender to encode data to many receivers by identifying the receiver`s identities. Therefore, the Key Generation Center (KGC) will assign a secret key to proxy in order to convert the initial cipher text into encrypted cipher text. Later, the sender will send the encrypted cipher text to receiver in order to decrypt into original data.By consolidating these schemes, this paper proposes a versatile primitive referred to as KGC Proxy Re-Encryption scheme (KGC-PPRE) and formalizes its semantic security.We evaluate less computational costs by using this KGC-PRE technique.

Keywords: Proxy Re-Encryption (PRE), Identity-Based Encryption (IBPRE), Cloud Mail, Key Generation Center (KGC).

Introduction

A Proxy Re-Encryption [1] system permits the proxy to modify cipher texts encrypted under KGC secret key into the various cipher texts. Receiver will receive the secret keys from KGC to decrypt into original plaintext [7].Proxy re-encryption has several applications added to the previous proposals for email forwarding, secure network file storage, and play acting scientific discipline operations on storage restricted devices [5].Many different voluntary properties succeed in recent Proxy re encryption schemes. The Proxy re encryption theme is equipped with an additional property that the receiver of a cipher text is anonymous. The schemes succeed multi-use bi-directional re-encryption [5].A cipher text will be re-encrypted multiple times. Moreover, a re-encoding key realizes the bi-directional share between 2 users. Specifically,if sender assigns a re-encryption key to a proxy for re-encrypting her cipher texts to receiver. The re-encryption key may alter to re-encrypt receiver's cipher texts to sender. These twoProxy re encryption schemes are provably secure below the chosen-cipher text attack severally within the random oracle and customary models. In distinction, the Proxy re encryption theme is multi-use unidirectional Proxy re encryption schemes within which bi-directional re-encryption is out. The recent revocable IPRE supports user revocation and delegation of cryptography rights at first Blaze [1] introduced the concept of proxy re-encryption named to as atomic proxy encoding in [1].

In 2003, Ivan and Doris [2] planned a unidirectional PRE by ripping the sender's secret key into 2 different elements then distributing to the proxy and receiver.Shamir[3] introduced an identity based mostly Proxy re encryption theme, during this theme email addresses or IP address be used to type public keys for users.

In identity-based mostly coding, the senders encode messages using the recipient's identity (a string) because of the public key. As an example, the sender may encode a message for Bob by using their email address. The identity based mostly proxy re-encryption schemes permits a proxy to convert an encoding below receiver's identity into one computed below sender's id. Inexperienced et al introduced the identity based mostly proxy re-encryption (IB-PRE) theme by incorporating the idea of Proxy re encryption and ID-based encoding. The PRE theme planned is unidirectional, multi-use and non-interactive. However, it's not collision-resistant.

Jean Weng[6]introduced the Conditional proxy re-encryption (C-PRE).The C-PRE theme consists of 3 principles: a sender, a proxy, and a receiver. A message is distributed to the sender with condition c is

encrypted by the sender using each public key and c.These keys are often generated by the sender and form the key trap-door Proxy re encryption and Identity Proxy re encryption permit just for one receiver. In contrast, BPRE permits a sender to come up with an initial cipher text to a receiver set, instead of one receiver, whose cipher texts are transformed from one user to another.

If the sender wants to share some data related to condition with different receivers. Then the sender will send the cipher text to proxy for Re-Encryption. Then the proxy will re-encode the cipher texts matching the condition to the receiver set. The receivers who want to access the file for decoding the cipher text, they request the secret keys to KGC. Using those secret keys receivers will decrypt the file.

This paper is organized as Section I gives an Introduction, Section II provides the literature survey. Section III provides the KGC-PRE system model. Section IV provides Secret Key Generation, Section V discusses the performance analysis and results, and FinallySection VI concludes the paper.

Literature Survey

The first PRE [1] was initiated within the accepted public-keysetting that incurs complex certificate Management. The PRE schemes solely permit knowledge sharing during a coarse-grained manner [6].That is, if the user assigns a re-encryption key to the proxy, all cipher texts are often re-encrypted then be accessible to the supposed users, else none of the cipher texts is re-encrypted or accessed by others. An Identity basedsystem [2] fewer well-organized in the side of communication and no more real in user occurrence.Users do not able to share the encrypted information to others, because of great extent issue is occurring. No Identity key is provided to cipher information

Proxy Re-Encryption [1] and, Identity-Based Encryption [2] permits one receiver. To handle this issue, the idea of broadcast PRE [4] has been planned. Broad cast PRE works during a similar method as Identity based PRE. In variance, Broad cast Proxy Re-Encryption permits a sender to come up with an initial cipher text to a receiver set, as a substitute one receiver. Further, the sender will delegate a key agree with another receiver.

A recent conditional proxy broadcast re-encryption theme [3] permits the senders to manage the time to re-encrypt their initial cipher texts. This demand makes this theme unnatural for the memory-limited or mobile senders and well planned just for special applications.

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 KGCproxy re encryption scheme with similar works and the comparison confirms the advantages of our KGC-PRE scheme. We built the encrypted cloud email system based our proxy re encryption scheme

In a proxy re-encryption system, a trustworthy key generation center (KGC) initializes the system values and generates secret keys. Later, if the sender additionally wishes to share some data related to constant condition with different receivers. Then the sender will deliver the cipher text to proxy for Re-Encryption. The receivers request the secret keys to KGC [7]. Using those secret keys receivers will decrypt the file.

3. KGC-PRE

Figure:1 Architecture

If the data owner intends to share the sensitive data stored in the cloud with another granted user. It is desirable that the requested data can be accessed by nobody other than receiver. Inspired with primitive of Proxy Re-Encryption, Sender can encrypt the sensitive data under her identity key which is generated by KGC and send to the proxy .The proxy will re encrypt the cipher text and will request the key to KGC ,and send to user. The sender will send the data to receiver.KGC will generate the secret keys to receiver for decrypting the data and re-decrypting data. The secure sharing based on PRE is illustrated in the Figure 1.

Cloud mail

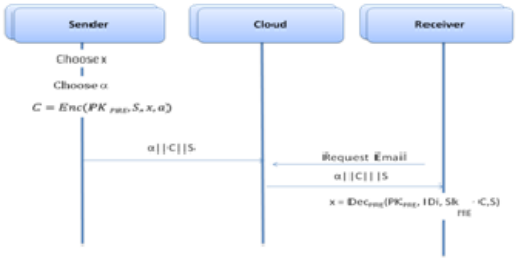

Figure: 2 Cloud Mail

The KGC generates the system parameters to initialize the Conditional-based cloud email system. It chooses a security value and runs a Setup PRE to generate secret keys as shown in figure 2.It chooses a secure symmetrical key encoding theme, i.e. AES Key Management: once a new user joins this technique, the KGC generates a private key for him. let ID denote email id new user. The KGC runs algorithm Extract PRE (MK_{PRE}, ID) to generate the private key SK_{ID}PRE, and sends it to the user in a secure channel and send an Encrypted data. A user can send an encrypted data to other users. And this email will be stored in the cloud server. It permits a user to share their outsourced encrypted information with others during a fine-grained manner. All Proxy re encryption users take their identities as secret keys to encode information and keep away from a user to fetch and verify alternative usersdata before encrypting his knowledge.

4. SECRET KEY GENERATION

- $Setup_{PRE}(\lambda,N)$: Given a security parameter λЄN and value N, this algorithm outputs a secret key SK_{PRE}.
- $Extract_{PRE}(_{PRE,}$ ID): Given SK_{PRE} and an identity ID, this algorithm outputs the SK^{ID}_{PRE} .

- $Enc_{PRE}(PK_{PRE,}S,m)$: Given PK_{PRE}, a set S of identities ,a plaintext m,this algorithm gives an initial cipher text C.
- $Re\text{-}Enc_{PRE}(PK_{PRE,}c)$: Given PK_{PRE}, a set S of some identities ,a cipher text,this algorithm outputs an initial ciphertext C`.
- $Dec\text{-}1_{PRE}(PK^{ID}_{PRE},SK^{ID}_{PRE},C`,S)$: Given PK_{PRE}, an identity ID and its secret key SK^{ID}_{PRE}, an initial cipher text C``, and a set S of some identities, this algorithm gives an plaintext.
- $Dec\text{-}2_{PRE}(PK^{ID}_{PRE,}SK^{ID}_{PRE,}C``,S)$: Given PK_{PRE}, an identity ID and its secret key SK^{ID}_{PRE} ,a re-encrypted ciphertext C`,this algorithm gives an plaintext.

5. PERFORMANCE ANALYSIS

When we compare our KGC-PRE scheme with existing CIBPRE scheme, Table: 1 summarizes the number of expensive algebraic operations. It shows that our KGC-PRE scheme is more efficient than CIBPRE scheme**.**

Algorithm	**CIBPRE**			**KGC-PRE**		
	BM	ME	MI	BM	ME	MI
ENC_{PRE}	1	r+7	1	0	3r+2	1
$DEC1_{PRE}$	2	r-1	2	2	r	2
KEY EXTRACT	0	2r+7	1	0	r+6	1
$RE\text{-}ENC_{PRE}$	8	R	2	2	r	1
$DEC2_{PRE}$	4	3r+2	4	3	r	2

Table: 1 the complexity of algorithms

BM=Bilinear map

ME=modular exponentiation

MI=modular Inversion

Algorithm	**CIBPRE**	**KGC-PRE**
Setup	$t_m + t_b$	$2n\ t_m$
KeyGen	$2t_m$	tm
Enc/ Encrypt	$ta+(8 + r)t_m$	$(r + 4)t_a+5t_m+t_b$
RkGen	t_m	$(r + 6)t_a+7t_m+t_b$
ReEnc	t_b	$(r + 1)t_a+t_b$

Dec1	$tm+t_b$	$(r + 2)t_a+2t_b$
Dec2	$(r + 1)t_a+$ $(r+1)t_m+2t_b$	$(r + 3)t_a+3t_b$
Sum	$(r + 2)t_a+$ $(r + 13)t_m+5t_b$	$(5r + 16)t_a+$ $(2n + 13)t_m+8t_b$

Table: 2 comparisons of computational costs between CIBPRE and KGC-PRE

Table I lists the computational costs comparison of the proposed IPRE scheme, CIBPRE [3] scheme and KGC-BRE scheme. It can be seen from the table that, for IPRE scheme, the computationalcosts of all algorithm are irrelevant to the size of complete users set, and only ”Enc” and ”Dec2” are linearly related to the size of target usersset; while, for CPBRE scheme,the computational costs of the ”setup” algorithm is linearlyassociated with the size of complete users set, and all otheralgorithms except ”KeyGen” are linearly correlated with thesize of target users set. On the other hand, except the efficiencyof”KeyGen”, ”Enc” and ”Dec2 / Decrypt-II” of IPRE are lesser than that of CIBPRE scheme.

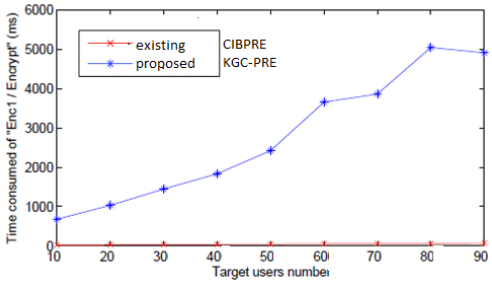

Figure: 3. Time consumed for Encryption

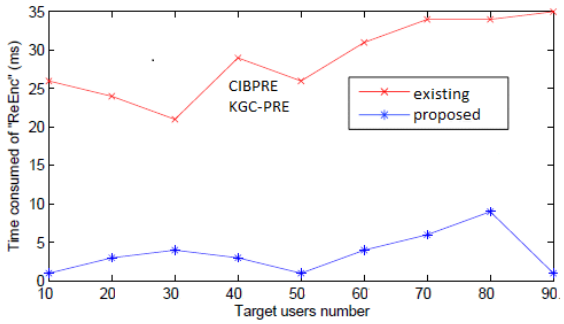

Figure: 4. Time Consumed For Re-Encryption.

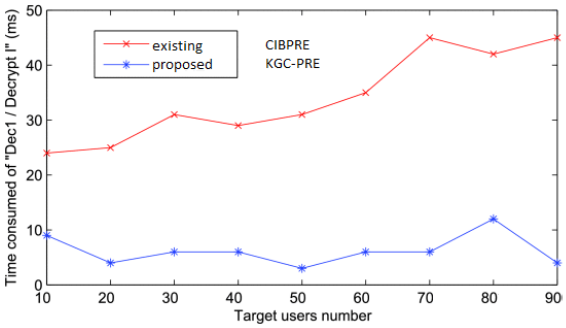

Figure: 5. Time consumed for Decryption

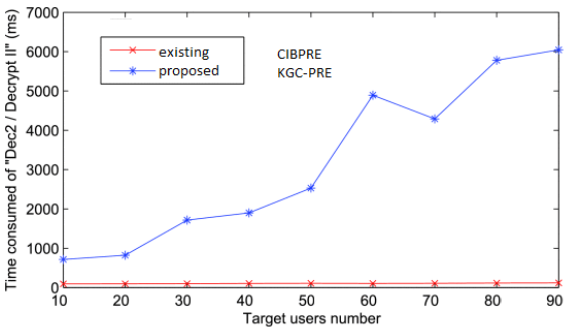

Figure: 6 Time consumed for Re- Decryption

It can be seen from Fig.4 and Fig. 5 that the time consumed of ”Encrypt” and ”Decrypt II” of CIBPRE scheme are less than the proposed IPRE scheme. For time consumed of ”Encrypt” and ”Decrypt II” algorithms. While in Fig. 6 and Fig. 7 that the time consumed of ”Dec1” and ”ReEnc” of the proposed KGC-PRE scheme are less than the counterparts of CIBPRE scheme.

We proved a formula for lesser costs and more secure, computes a k`=c3/h (k) and finally gives a plaintext.

K= (e(c1,h^Δγ $^{(ID1,S1)}$).e(SK^{id1}_{PRE},C2)) with following equation.

Δγ(ID,S)=γ-1(idi€s ^id i≠id (γ+h(idi))- (idi€s ^ idi≠id (γ+h(idi))

Conclusion

Finally, we propose a tendency to compare the projected Conditional identity based proxy re-encryption scheme with similar works and therefore the comparison confirms the benefits of our KGC identity. We designed the encrypted cloud email system primarily based our KGC-PRE scheme. Compared with the previous techniques like PGP and IBE, Our Proxy Re- Encryption-Based system is way a lot of economical within the facet of communication and a lot of sensible in user expertise.

References

1. Blaze, M. G. Bleumer, and M. Strauss. (1998). Divertible protocols and atomic proxy cryptography,” in Proc. Int. Conf. Theory Appl. CrytographicTechnology.: Adv. Cryptol, 127–144.
2. Shamir, A. Palacio and B. Warinschi. (2007). A Closer Look at PKI: Security and Efficiency. Proc. PKC 2007 Springer, Heidelberg, 458-475.
3. Shao, G. Wei, Y. Ling, and M. Xie (2011). Identity-based conditional proxy re-encryption in Proc. IEEE Int. Conf. Commun., 1–5.
4. Chu, C.K. J. Weng, S. S. M. Chow, J. Zhou, and R. H. Deng. (2009). Conditional proxy broadcast re-encryption in Proc. 14th Australasian Conf. Inf. Security Privacy, 327–342.
5. Zhiguang Qin, Hu Xiong, Shikun Wu, and Jennifer Batamuliza. (2014). A Survey Of Proxy Re-encryption For Secure Data Sharing In Cloud Computing. Journal Of Latex Class Files, 13(9)
6. PengXu, Member, IEEE, Tengfei Jiao, Qianhong Wu, Member, IEEE, Wei Wang, Member, IEEE,Hai Jin, Senior Member, IEEE” Conditional
7. Identity-based Broadcast ProxyRe-Encryption and Its Application to Cloud Email”
8. Green, M., and G. Ateniese. (2007). Identity-based proxy re-encryption in Proc. 5th Int. Conf. Appl. Cryptography Netw. Security, 288–306.

R.Bhagya sri, student Pursuing M.Tech in computer science and engineering from G. Pulla reddy engineering college, kurnool affiliated to Jawaharlalnehru technological university, Anantapur, AP, 515002 India

Dr.G.Vijay Kumar, Associate professor in computer science and engineering dept., GPREC kurnool, AP 518007, India, Research Interest in the areas of Wireless Mesh Networks, Mobile Ad Hoc Networks, Cross Layer Design, Power Conservation Protocol Design.