# SECURED EMAIL BROADCASTING USING IDENTITY BASED ENCRYPTION

R.Bombale[1], Prof.S.M.Rokade[2]
[1] *M.E., Computer Engineering Department, Maharashtra, India*
[2] *HOD, Computer Engineering Department, Maharashtra, India*

## ABSTRACT

*Identity based proxy encryption is based on Proxy Re-encryption (PRE). It formalizes semantic security. The number of extended proxy re-encryption schemes have been proposed such as conditional identity based PRE (CIBPRE), Broadcast PRE (BPRE). Conditional IBPRE allows sender to encrypt message and send it to multiple users or receivers by specifying their identities. Data encryption keys are given to proxy server by which proxy can re-encrypt into new one and predetermined receivers. Furthermore, re-encryption keys are associated with some condition is such way by matching ciphertexts can be re-encrypted. With proposed approach sender can enforce his control on his remote ciphertexts in a fine-grained manner. Proposed CIBPRE is provable secured as ciphertexts get re-encrypted and its keys are of constant size. Along with CIBPRE scheme, email broadcasting with group of user is contributed. It decreases the time required for data encryption as well as re-encryption. With experimental results we have to show that the proposed system is time efficient as compared to previous system.*

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

## 1. INTRODUCTION

To outsourced and share the data securely proxy re-encryption (PRE) scheme is used. It is more secured and flexible method for data storing and sharing. Using public key, user data get encrypt and then it is outsourced to cloud server. After deciding receiver re-encryption keys associated with receiver delegated to proxy server. Proxy server re-encrypts the initial ciphertexts. Previous methods of PRE uses complex certificate management approach [2]. Certificate management is a crucial problem hence to address this problem several researches have been conducted. Identity based proxy re-encryption i.e. IBPRE is used to recognize an identity of receiver to relieve the problem of identity based proxy re-encryption. A previous technique of proxy re-encryption such as, PRE and IPRE allows a single server. It creates problem when there are multiple receivers which tends to invoke PRE and IPRE multiple times. To overcome the problem of single server BPRE scheme is proposed in [9]. It is more versatile than the PRE & IPRE. It allows broadcasting of initial ciphertext to group of receiver's. Moreover, sender delegates re-encryption keys with another receiver set. This is coarse gained control strategy which limits the application of PRE systems. To overcome this issue, CPRE scheme is proposed which is referred as, Conditional proxy re-encryption. It enforces fined-grained re-encryption control over on initial ciphertexts. In this scheme, by associating some condition better re-encryption is achieved. Conditional proxy re-encryption allows sender to control the time re-encryption on their ciphertexts.

In proposed conditional identity based proxy re-encryption (CIBPRE) scheme, KGC i.e Key Generation Center is introduced and it initializes the attributes for CIBPRE. It also generates private keys for users. In this scheme, files are encrypted using identities of receiver as well as file sharing conditions. Sender can also share some files associated with similar condition with other users or receivers. Then label of re-encryption keys with conditions are delegated to proxy. Attributes used to generate re-encryption keys are separate for each individual receiver. In proposed system, authorized receiver can decrypt file using private keys and saved to its end. Also newly authorized user or receiver can also decrypt re-encrypted ciphertexts using private keys. Ciphertexts are saved remotely in secured way. Cloud email system: It is promising application which permits enterprises to pay for services of cloud i.e. SaaS and developer their own email system. It is cheaper as well as scalable than traditional un-precise solution. To estimate the quantifiable cost savings of cloud systems, Proofpoint Group is used as an economic model [1]. It evaluates the expenses for both systems at the time of retrieval and the time of software license period.

## 2. RELATED WORK

M. Blaze, G. Bleumer and M. Strauss [2], introduced a notion of divertibility as a protocol property. It is opposed to the existing notion as property of language. In this paper, author introduced atomic proxy

cryptography in which an atomic proxy function, in conjunction with a public proxy key, converts ciphertexts (messages or signatures) for one key into ciphertexts. Once the proxy keys are generated they applied in untrusted environments. They have also represented an atomic proxy functions for discrete-log-based encryption, identification, and signature schemes. With the proposed scheme, there is no approximate visualization for existence of an atomic proxy functions in general for all public-key cryptosystems.

G. Ateniese, K. Fu et al. [3], also proposed an atomic proxy re-encryption technique. It has secure re-encryption; therefore it can manage encrypted files and predict that fast. In this paper a bilinear map is used for improved re-encryption scheme. One of the most promising applications for proxy re-encryption is giving efficiency of proxy to the key server of a confidential distributed file system; using such way server not required to be completely trusted with all keys of the system and the secret storage for each user can also be reduced.

M. Green and G. Ateniese[4], represented a new construction for enabling non-interactive , unidirectional proxy re-encryption in the IBE settings. This scheme is efficient and can be deployed within standard IBE framework. Author mainly proposed an interesting problem to find an efficient construction for multiuse CCA-secure IBE-PRE scheme. T. Matsuo [5], proposed two new proxy re-encryption schemes. One for the decryption right delegation from PKE user to IBE users whereas, the other is for delegation among IBE users. In this paper proposed system is based on dBDH assumption. A chosen ciphertext security for identity based system is proposed in [6]. It is proposed for random oracle model assumption variants of the computational Diffie-Hellman problem. This system is based on bilinear map groups. Weil pairing on ecliptic curves is one of the examples of such map.

In [7], author tackles the problem of how to control the proxy in PRE systems at a fine-grained level. A conditional proxy re-encryption is introduced for this. A CCA-secure C-PRE used as security notions and also proposed CPRE scheme support multiple conditions with reasonable overhead.

A type-and-identity-based proxy re-encryption scheme based on the Boneh-Franklin scheme is discussed in [8]. It has been proved semantically secure against a chosen plaintext attack. In this, delegators have privileges to provide different re-encryption capabilities to the proxy while using the same key pair. Such property is useful in PHR disclosure scheme where an individual can easily implement fine-grained access control policies to his PHR data. For future work, it would be interesting to construct type and identity-based proxy re-encryption schemes with chosen ciphertext security and to investigate new applications for this primitive.

G. Ateniese, K. Benson, S. Hohenberger[9], proposed key-private (or anonymous) re-encryption keys as an additional useful property of PRE schemes. They were formalized the notion of key-privacy for proxy re-encryption schemes, where even the proxy performing the translations cannot distinguish the identities of the participating parties. Their construction realizes CPA security. A simpler key-private PRE schemes can be devised, although at the cost of stronger assumptions. Furthermore they have extended their work in future for DBDH and the Decision Linear assumptions used here are actually quite mild. Nevertheless, finding more efficient schemes, even under stronger assumptions or in the random oracle model, would be quite useful for several applications.

T. Matsuda, R. Nishimaki , and K. Tanaka[10], proposed Proxy re-encryption (PRE) is a cryptographic application. It is an encryption system with a special property. A semi-honest third party is able to re-encrypt ciphertexts for one user ‘X’ into other ciphertexts for the other user ‘Y’ without using original user’s ‘X’ secret key. They classify PRE into bidirectional and unidirectional schemes. The PRE-CCA security bidirectional or unidirectional scheme also discussed.

K. Liang, J. K. Liu et al [11], discussed about Identity-based encryption (IBE). It eliminates the necessity of having a costly certificate authentication process. However, revocation remains as a uncertain task in terms of ciphertext renovation and key update phases as due to the lack of a certificate revocation list in this infrastructure. They have proposed the first cloud-based revocable identity-based proxy re-encryption (CR-IB-PRE) scheme. With the user revocation facility it also delegates the decryption rights. No matter a user is revoked or not, at the end of a given time period the cloud behave like a proxy will then re-encrypt all ciphertexts of the user under the current time period to the next time period. If the user is revoked in the upcoming time period, he cannot decrypt the ciphertexts by using the expired private key anymore. This scheme only required PKG to publish constant-size key update information for all non-revocable users once at the beginning of each time period.

D. Boneh and X. Boyen[12], constructed two Identity Based Encryption (IBE) systems that are selective identity secure without the random oracle model in combined rigged with a bilinear map. Selective identity secure IBE is a slightly weaker security model than the standard security model for IBE. The first construction is based on the now classic BDH assumption. It extends readily to give a selective identity HIBE without

random oracles that can efficiently be made chosen ciphertext secure and the second construction is based on the Bilinear Diffie-Hellman Inversion assumption. However, this system is quite impractical and should only be viewed as a constructive proof that such constructions are indeed possible.

## 3. PROBLEM DEFINITION

To design and develop a secured group email broadcasting system using Identity based re-encryption.

## 4. PROPOSED SYSTEM

In proposed work, we are going to develop an encrypted cloud email system with CIBPRE. It is combination of IPRE and CPRE scheme. From analysis of literature survey we found that CIBPRE-based system is implementation-friendly and more efficient in communication than existing approaches such as pretty good privacy (PGP) or IBE.

In PGP or IBE schemes sender must fetch the historically encrypted email from the cloud and decrypt it, and then re-encrypt it again to these receivers one by one which is not convenient task. Therefore we have proposed A Fine-Grained Approach for Unified Group Email Broadcasting Using Identity Based Encryption.

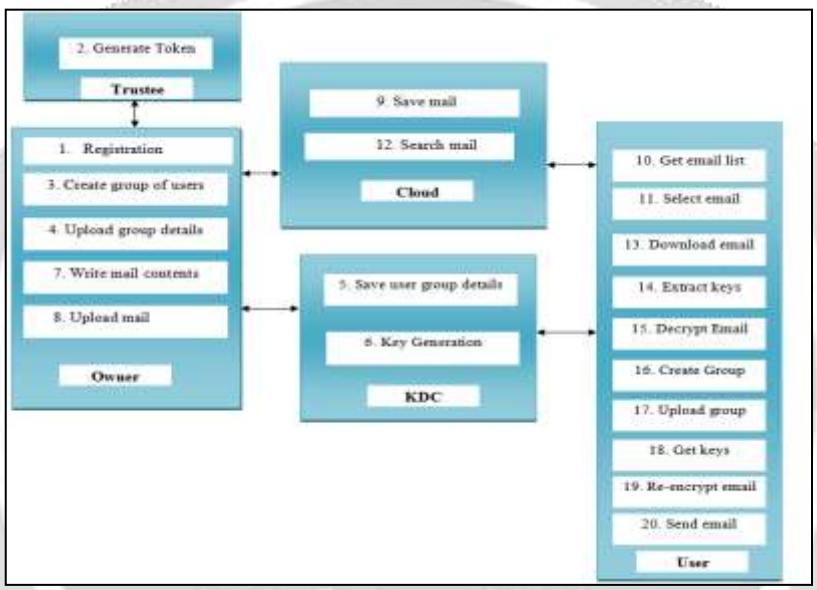


**Fig -1**: System Architecture

**1. Data owner (Sender):**

1. Registration on trustee

2. Get Token from trustee after successful registration.

3. Create group of users.

4. Upload group details on KDC server.

5. Get keys from KDC.

6. Extract keys.

7. Write mail content and encrypt them. 8. Upload mail on cloud.

9. Get notification of saved mail.

**2. Trustee:**

1. Validate and save user details.

2. Generate token.

3. Verify user details at the time of user login.

**3. KDC (Key Distribution Center) server:**

1. Save user group details.

2. Generate key and send to it valid user.

**4. Cloud:**

1. Save mail.

2. Search mails.

**5. User:**

1. Request for cloud to show inbox.

2. Get email list from cloud.

3. Select email.

4. Request for cloud to download email.

5. Request for KDC to get key.

6. Extract key.

7. Decrypt mail.

8. View mail.

9. Create group.

10. Upload group details on KDC server.

11. Get keys from KDC.

12. Extract keys.

13. Reencrypt mail contents.

14. Upload mail on cloud.

## 5. ALGORITHMS

### 5.1 AES Algorithm:

**Input:**

Plain text message m in Byte [] , Key k

**Output:**

Cipher text message in byte []

**Processing:**

1. Define 4 * 4 state array
2. Define constant Nr = 4, R=16
3. Copy m in state[]
4. Add each byte of state[] to key k using ⊕
5. For Nr-1 rounds
   Replace every byte in state[] with new value using lookup table

   Shift last 3 rows of state[] upside cyclically

   Combine last 4 columns of state[]

   Add each byte of state[] to key k using ⊕

   end For
6. Shift last 3 rows of state[] upside cyclically
7. Add each byte of state[] to key k using ⊕
8. Copy State[] to output[]

**5.2. AES Decryption:**

**Input:** Cipher text message C in byte [], Key k

**Output:** Plain text message m in Byte []

**Processing:**

1. Define 4 * 4 state array
2. Define constant Nr = 4, R=16 ,
3. Copy C in state[]
4. Add each byte of state[] to key k using ⊕
5. For Nr-1 rounds Inverse Replace every byte in state[] with new value using lookup table Inverse Shift last 3 rows of state[] downside cyclically combine last 4 columns of state[] Add each byte of state[] to key k using L end For
6. Inverse Shift last 3 rows of state[] down word cyclically
7. Inverse Add each byte of state[] to key k using ⊕
8. Copy State[] to output[]

## 6. MATHEMATICAL MODEL

**For Trustee:**

**TI: Trustee Input**

**TI= {TI1, TI2}**

TI1- User registration request

TI2- User login request

**TF: Trustee Function**

**TF= {TF1, TF2}**

TF1= Response to the user after successful registration

TF2= Get login details and generate token

**TO= Trustee Output**

**TO= {TO1, TO2}**

UO1= successful registration response

UO2= User token

**For KDC:**

**KI: KDC Input**

**KI= {KI1, KI2}**

KI1- User token

KI2- Accessing rights

**KF: KDC Function**

**KF= {KF1, KF2, KF3}**

KF1= Key Generation

KF2= Group creation

KF3= Key Distribution

**KO= KDC Output**

**KO= {KO1, KO2}**

KO1= Master Key

KO2= Re-encryption keys

**CI: Cloud Input**

**CI= {CI1, CI2, CI3, CI4}**

**C**I1- Encrypted email from user

**C**I2- Email access rights

**C**I3- User token

**C**I4- Request of file downloading

**CF: Cloud Function**

**CF= {CF1, CF2, CF3, CF4, CF5, CF6}**

**C**F1= Save Email

**C**F2= User verification

**C**F3= Respond to file downloading request

**CO= Cloud Output**

**CO= {CO1, CO2, CO3}**

**C**O1= Email saved on cloud

**C**O2= Get saved email

**C**O3= Update users rights

**UI: User Input**

**UI= {UI1, UI2, UI3, UI4}**

UI1- User registration details

UI2- User login Details

UI3- User email

UI4- Access Rights

UI5- Email downloading request

**UF: User Function**

**UF={UF1, UF2, UF3, UF4, UF5, UF6,UF7}**

UF1= User Registration and token generation

UF2= User Authentication and Token Retrieval

UF3= Generate keys

UF4= Email Encryption with receiver's identity

UF5= Upload email

UF6= Download email from server

UF7=Decrypt email using re-encryption keys

**UO=Output**

**UO= {UO1, UO2, UO3}**

UO1= Token

UO2= Encrypted email

UO3= original email after decryption

## 7. EXPERIMENTAL SETUP

System is implementing using java platform. Cloud server provides web services to the user system. User can be owner or data user. Swing components are used to designed user system. For communication at user's end HTTP is used.

Data is stored in MySQL database. To handle multiple user requests, Apache tomcat server is used to at server end. For development of system, Eclipse and netbean-8.1 IDE is used.

**Dataset used:-**
Synthetic Dataset: For email data sharing text as well as other multimedia files are used. Different files of various sizes ranging from 100 bytes to 2 MB are collected.

## 8. RESULT TABLES AND DISCUSSION

For secured data sharing encryption is used. In this system user identity hiding mechanism is proposed using which user can hide his/her identity from cloud. The cloud registration is done using token. Trustee system is responsible for token generation. Approximate 140 ms are required for token generation for each user.

For all multimedia files such ad text, pdf, images, audio, video files, the processing time is captured for various file sizes. Following graph represents the time required for Encryption and Decryption of files form 1 mb to 5 mb.

**Table-1:** Efficiency Evaluation

| File Size(In KB) | Encryption Time(in Sec) | Decryption Time(In Sec) |
|---|---|---|
| 1 | 2.8 | 1.62 |
| 2 | 3.9 | 2.16 |
| 3 | 4.21 | 3.12 |
| 4 | 4.49 | 3.85 |
| 5 | 5.1 | 4.34 |

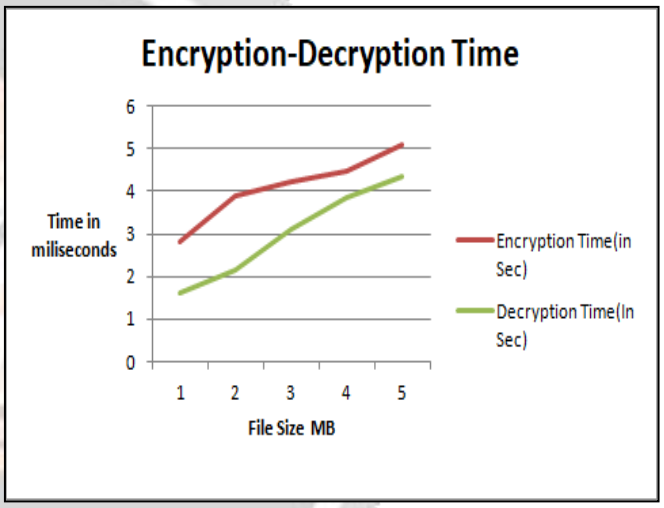


**Chart-1:** Efficiency evaluation

User identity is used to for key generation. For key processing, key generation, key extraction rekey encryption rekey decryption time is calculated as per the user count. As number of users increases the time required for key processing also increases.

**Table-2:** Time evaluation for Image files

| No of Share Users | Key Gen Time | Key Extraction | Re-Key-encryption Time | Re-Key-decryption Time |
|---|---|---|---|---|
| 4 | 0.234 | 0.421 | 0.4321 | 0.682 |
| 8 | 0.37 | 0.623 | 0.6832 | 0.785 |
| 12 | 0.68 | 0.843 | 0.892 | 1.03 |
| 16 | 0.84 | 1.06 | 1.12 | 1.29 |

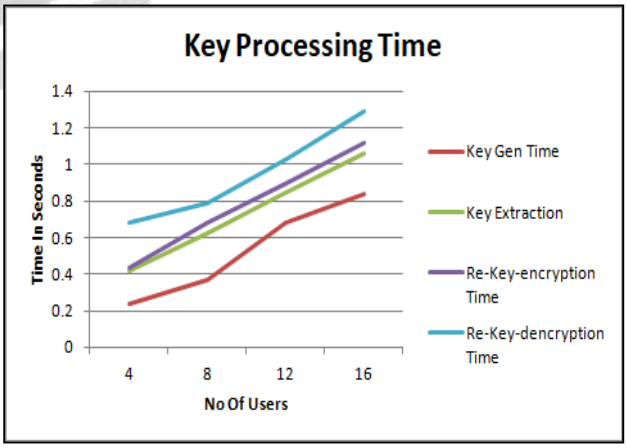


**Table-3**: Key generation

| No of Users | Key Gen Time | Key Extra-ction | Key Gen Time(Group Creation) | Key Extraction (Group Creation) |
|---|---|---|---|---|
| 4 | 0.234 | 0.4 | 0.15 | 0.2 |
| 8 | 0.37 | 0.6 | 0.17 | 0.3 |
| 12 | 0.68 | 0.8 | 0.16 | 0.3 |
| 16 | 0.84 | 1.1 | 0.18 | 0.2 |

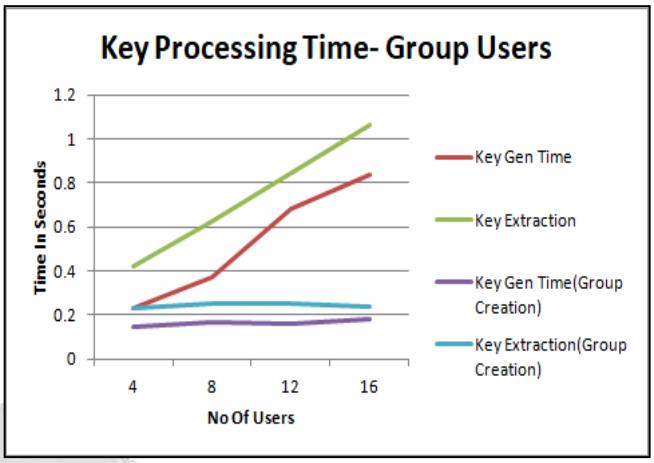


**Chart-3**: Key processing(group users)

Rather than using individual identity of user, multiple users are grouped together and assigned a single group identity. For key generation group id as a single identity is used. The time required for key processing is now independent of number of users present in a group. The time required for key processing is equivalent to the time required for key processing using identity of single user.

## 9. CONCLUSIONS

Conditional identity based broadcast PRE (CIBPRE) and formalizes its semantic security is discussed in this paper. There are two entities in the proposed approach namely sender and receiver. A sender can create group in which he/she have to broadcast email, then KDC will provides encryption keys for email encryption which can be extracted by sender. These keys are used to encrypt email and send by sender over cloud. At the receiver end he/she can download and decrypt email with the help of keys. CIBPRE receiver can re-encrypt mail and can send it to other users group which is created by him using his/her reencrypted keys. Hence, proposed method allows a user to share their outsourced encrypted data with others in a fine-grained manner. It is unidirectional approach of secured email broadcasting. It is feasible to manage encrypted files stored on distributed, trusted replicas.

## 10. ACKNOWLEDGEMENT

## 11. REFERENCES

[1] Peng Xu, Tengfei Jiao, Qianhong Wu," Conditional Identity-Based Broadcast Proxy Re-Encryption and Its Application to Cloud Email", IEEE transaction on computers, vol 65, No.1, January 16.

[2] 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.

[3] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved proxy reencryption schemes with applications to secure distributed storage," ACM Trans. Inf. Syst. Security, vol. 9, pp. 1–30, 2006

[4] K. Liang, J. K. Liu, D. S. Wong, and W. Susilo, " An efficient cloud based revocable identity-based proxy re-encryption scheme for public clouds data sharing," in Proc. Eur. Symp. Res. Comput. Security, 2014, pp. 257–272.

[5] T. Matsuo, "Proxy re-encryption systems for identity-based encryption," in Proc. 1st Int. Conf. Pairing-Based Cryptography, 2007, pp. 247–267.

[6] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," in Proc. 21st Annu. Int. Cryptol.: Adv. Cryptol., 2001, pp. 213–239

[7] 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.

[8] 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.

[9] G. Ateniese, K. Benson, and S. Hohenberger, "Key-private proxy re-encryption," in Proc. Cryptographers' Track RSA Conf. Topics Cryptol., 2009, pp. 279–294.

[10] T. Matsuda, R. Nishimaki, and K. Tanaka, "CCA proxy re-encryption without bilinear maps in the standard model," in Proc. 13th Int. Conf. Practice Theory Public Key Cryptography, 2010, pp. 261–278.

[11] K. Liang, J. K. Liu, D. S. Wong, and W. Susilo, " An efficient cloudbased revocable identity-based proxy re-encryption scheme for public clouds data sharing," in Proc. Eur. Symp. Res. Comput. Security, 2014, pp. 257–272.

[12] D. Boneh and X. Boyen, "Efficient selective-id secure identitybased encryption without random oracles," in Proc. Adv. Cryptol., 2004, pp. 223–238.