# A Review on Fine-Grained Approach for Unified Group Email Broadcasting Using Identity Based Encryption

[1]R. L. Bombale, [2]Prof. S.M.Rokade
[1]PG student, [2]Head of Department
[1]Computer Engineering Department, SVIT, Chincholi, Sinner, Nashik, India

***Abstract*** **- Previous techniques of certificate verification such as, pretty good privacy protocol and identity-based encryption (IBE) are unsuitable for updating the ciphertexts and keys. Both techniques were used for emailing security purpose. But these techniques preserve the security of cloud email but their performance is less efficient due the linear size with the number of receivers. Also they required certificate verification of the receiver from security point of view. A proxy re-encryption technique based on Identity-based broadcast encryption i.e. CIBPRE scheme. Re-encryption key associated with the condition such that only matching ciphertext can be re-encrypted. It allows the original sender to enforce access control over his remote ciphertext in fine-grained manner. In this paper we are contributing ourselves for user group creation for sharing data with them at same time by which encryption & re-encryption time can be decreases as compared to previous system.**

***IndexTerms*** **- Proxy re-encryption, cloud storage, identity-based encryption, broadcast encryption**

## I. INTRODUCTION

PRE is proxy based re-encryption technique. It integrates the benefits of IPRE i.e. Identity based proxy re-encryption, CPRE, BPRE scheme for more flexible applications. The PRE scheme proposed in the public key infrastructure incurs complicated certification management. To relieve this problem an identity based re-encryption (IPRE) scheme is implemented [11]. Instead of fetching certificates for verifying receiver's identity the proxy just needs receiver's identities. Another problem occurs when there are more receivers the system needs to invoke PRE and IPRE many times hence the concept of broadcast has been proposed i.e. BPRE. It is more versatile than the PRE and IPRE scheme. BPRE allow sender generate initial ciphertext for the entire receiver instead of single receiver. The proxy can re-encrypt all initial ciphertexts or none of them. There is limitation for proxy-re-encryption is the control of coarse-gained over ciphertexts to re-encryption. To overcome such limitation CPRE scheme is proposed. CPRE is conditional proxy re-encryption, in which ciphertext meeting specified condition can be re-encrypted by proxy while holding corresponding re-encryption keys. Integrating this entire scheme a CIBPRE scheme is introduce in [2]. System parameters are initialized by the key generation center (KGC). It also generates the private key for users. Everyone is aware with concept of data encryption before upload it on cloud. Proposed CIBPRE encrypts the file with the receiver's identity and the file-sharing condition. Sender can delegate a re-encryption key labeled with the condition to the proxy, and the parameters to generate the re-encryption key, if he wants to share a file with same condition to the other receiver's. With CIBPRE, authorized receiver having private keys can decrypt initial ciphertexts and also newly authorized receiver can access file by decrypting initial ciphertext matching condition to the resulting receiver set. As initial ciphertext stored secretly, sender do not need to re-encrypt it repetitively. This feature can be versatile for secure remotely stored file. In experimental results, it seems that without considering private key one cannot learn anything about the plaintexts hidden in initial and re-encrypted CIBPRE ciphertexts. There is problem in an initial re-encryption if ciphertext and the key are belonging to different conditions. Selective-ID and Chosen Plaintext Attack (IND-sID-CPA) used for indistinguishability of conditions.

The proposed an efficient CIBPRE which is provably secure. Author proved IND-sIDCPA security of proposed CIBPRE, if the underlying identity-based broadcast encryption (IBBE) scheme is secure and the Decisional Bilinear Diffie-Hellman (DBDH) assumption holds [2]. CBPRE approach works on constant size initial and re-encrypted ciphertexts. CIBPRE scheme is more efficient than the previous techniques like, PGP and IBE. CIBPRE scheme is much more efficient aspect of communication and it is more practical as per the user experience.

## II. 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.

## III. PROBLEM STATEMENT

To address the problem of certificate verification of each receiver while transforming ciphertexts from one entity to another.

## IV. SYSTEM ARCHITECTURE

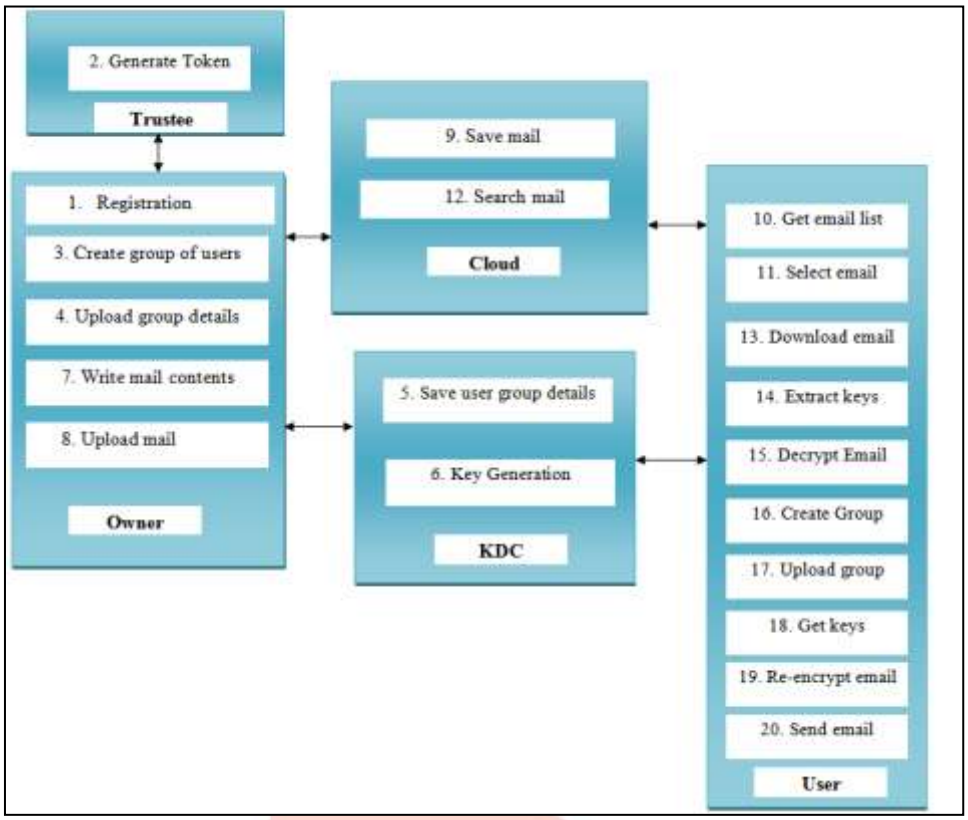


**Figure 1** System Architecture

Figure 1 represents the system architecture. As shown in figure there are five entities present in the proposed system. The responsibilities of each one in given as below:

Data Owner has responsibilities of registration on trustee by which he/she gets the token of authorization.

Trustee server will generate the token for user by validating his/her registration details.

Then he/she creates the group of users with whome he/she wants to share the data. This group is saved on KDC server and KDC will generate the keys for data encryption before uploading it on cloud. Data owner extract keys, write email contents then encrypt it by using secret key and upload encrypted data on cloud. At the cloud end data is saved.

End user or group of user can view inbox to get shared data or incoming email list. User can download email by selecting it and then decrypt with the help of keys which is given by KDC server as per user request for data downloading.

At the user's end, user can also create group and upload it on KDC server (Same like data owner). Get keys from KDC to re-encrypt data or email and again upload re-encrypted data on the cloud server.

## V. CONCLUSION

In this review paper, we have studied some existing techniques of proxy re-encryption. There have some problems or limitations in existing techniques such as, CR-IB-PRE supports for efficient user revocation but with the user revocation facility it also delegates the decryption rights. A well known scheme PRE cannot re-encrypt the initial ciphertext in a meaningful way. There have some complicated issues of certification management in the infra of cloud. A PRE and IPRE scheme does not have facility of group data sharing i.e. broadcasting. From literature survey analysis, we analyze that the integrated scheme called as, CIBPRE i.e. conditional identity-based broadcast PRE can be better solution to address all these problems that we discussed in this review.

## VI. ACKNOWLEDGMENT

I would like to express my special thanks to my project guide Prof. S.M.Rokade as well as other staff members of SVIT, Chincholi, Sinner, Nashik for their helpful guidance and co-ordination for this academic work. I special thanks to our principal Dr. S.A.Patil for their precious guidance

## REFERENCES

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.

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.

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

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.

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

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

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.

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.

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.