International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 04 Issue: 06 | June -2017 www.irjet.net p-ISSN: 2395-0072

# EFFICIENT REVOCATION AND SECURE ATTRIBUTE-BASED PROXY RE-ENCRYPTION SCHEME

**MAHESH S. GUNJAL[1], Dr. B. L. GUNJAL[2]**

*[1]PG Student, Dept. of Computer Engineering, AVCOE, Maharashtra, India*
*[2]Associate Professor, Dept. of Computer Engineering, AVCOE, Maharashtra, India*

---

**Abstract -** *This paper proposes a new Ciphertext-Policy Attribute-Based Proxy Re-Encryption (CP-ABPRE) scheme to integrating the dual system encryption technology and selectively secure access control policy as an enhancement to Circuit Ciphertext-policy Attribute-based Hybrid Encryption Model. While the introduced scheme supporting any standard access structures is built in the composite structure bilinear group, it is verified adaptively chosen Ciphertext Attack secure in the standard technique without threatening the expressiveness of access policy. In this paper, we attempt in addition to making an enhancement for the model to obtain more efficiency in the re-encryption key generation and re-encryption phases. Proxy Re-Encryption (PRE) is an effective cryptographic essential model that permits a data owner to nominee the access rights of the encrypted data which are stored on a cloud storage system to remaining entities without leaking the information of the data to the honest-but-curious cloud server. It implements the effectiveness for data sharing as the data owner even working with limited resource devices can offload most of the computational activity to the cloud. Since its establishment, many variants of PRE have been recommended and proposed. A Cipher text-Policy Attribute-Based Proxy Re-Encryption (CP-ABPRE), which is observed as a regular approach for PRE, engages the PRE technology in the attribute-based encryption cryptographic framework as like that the proxy is granted to make change an encryption down an access policy to another encryption under a new access policy. CP-ABPRE is suitable to real-time sharing secure data in the network or cloud applications.*

***Key Words***: Cloud Computing, Ciphertext-Policy Attribute Based Encryption, Proxy Re-Encryption, Attribute-Based Encryption, Cloud Storage, Circuits.

## 1. INTRODUCTION

In recent years, the Attribute-Based Encryption (ABE) scheme [1] has drawn the great attention of researchers to a development of Internet and open distributed Networks. The distinct of Public Key Encryption mechanism, ABE scheme takes attributes as the public key and associates the ciphertext and user's secret key with attributes, so that it provides more flexible access control mechanism over encrypted data. To perform the sending node's operation for fine-grained access control of data sharing and reduced the cost of network bandwidth. As a result, ABE has a broad prospect in the large-scale distributed applications to support one-to-many communication mode. There are two types of attribute-based encryption methods, are as follows:

- Key-Policy Attribute-Based Encryption (KPABE)
- Ciphertext Policy Attribute Based Encryption (CP-ABE)

In a Key-Policy Attribute-Based Encryption i.e. KP-ABE System, key distributor is the major part. The decision of access control policy is made by the key distributor instead of the enciphered, which having limited that is it controls the practicability and usability for the system in practical applications [8] in a Ciphertext-Policy Attribute-Based Encryption i.e. CP-ABE system, each ciphertext is related with an access structure, and each private key is given with a set of different attributes. A user is able to decrypt a ciphertext if the keys attribute set validates the access control structure relates with a ciphertext. However, CP-ABE is complementary, and the sender could specify access control policy so, compared with KP-ABE schemes, CP-ABE schemes are more suitable for the realistic scenes.

The ABE scheme has introduce the proxy Re-encryption scheme thus considering such a scenario, in the email forwarding, Alice is going on vacation and wishes the others like Bob could still read the message in her encrypted emails. With an Attribute-Based Proxy Re-encryption (ABPRE) system, in which a proxy is allowed to transform a ciphertext under a specified access policy into the one under another access policy, she could meet her intentions without giving her secret key to either the mail server or Bob. So ABPRE schemes [4] are needed in most of practical network applications, especially Ciphertext-Policy ABPRE (CP-ABPRE) schemes [5], which have more flexible access control policy than Key-Policy ABPRE (KP-ABPRE) schemes [4].

An ABPRE scheme has an authority, a sender, a user called delegator who needs to delegate his/her decryption ability

to someone else, a proxy who helps the delegator to generate a re-encrypted ciphertext, and some receivers as participants. It allows a semi trusted proxy to transform a ciphertext under an access policy to the one with the same plaintext under another access policy. ABPRE schemes were proven secure in the selective security model.

### 1.1 Our Contribution

In this work, we use the first construction of a ciphertext policy attribute-based Proxy Re-encryption scheme (CP_ABPRE) to relate integrating the dual system encryption technology and selectively secure access control policy. In our system, an access structure and an attribute set is required as auxiliary input to the re-encryption key algorithm; meanwhile, an attribute set is required in the input to the private key generation and decryption algorithms. So, Security concern we propose firstly create the selective access structure for ciphertext policy attribute base encryption and then used the chosen ciphertext security for proxy re-encryption scheme to integrating the dual system encryption technology.

The main objective of our paper is structured as follows. In Section 1 we discuss related work and give our construction that is proposed work. In Section 2 we define our project preliminaries. we then give our system model and security algorithm definitions in Section 4. We then present our implementation and performance analysis in Section 4. Finally, we conclude in Section 5.

### 1.2 RELATED WORK

In 2005, Sahai and Waters [16] proposed Fuzzy IBE (FIBE) which regards identities as a set of descriptive attributes. It is often regarded as the first concept of ABE [1, 18]. ABE can be categorized as either KP-ABE or CP-ABE, and the latter is more flexible and more suitable for the realistic scenes [2]. In 2007, Cheung and Newport [19] used AND gates on positive and negative to express attributes in order to achieve their CP-ABE scheme's access policy and proved the security under the DBDH assumption. And then Nishide et al. [20] designed a new CP-ABE scheme with AND gates on multi value attributes as its access policy.
In 2010, S. Yu, C. Wang, K. Ren, and W. Lou, worked on Attribute Based Data Sharing with Attribute Revocation. This paper use semi-trust able on-line proxy servers. This server enables the authority to revoke user attributes with minimal Effort. This scheme was uniquely integrating the technique of proxy re-encryption with CP-ABE, and also enables the authority to delegate most of laborious tasks to proxy servers.

In 2011,Waters [25] used Linear Secret Sharing Scheme (LSSS) access structure under *q*-PBDHE assumption to construct a CP-ABE scheme. In 2014, Garg et al. [29] constructed the first fully secure ABE scheme that can handle access control policies expressible as polynomial size circuits. Afterwards, some excellent adaptively secure ABE schemes were proposed. In 2013, Li [9] presented a new CP-ABPRE scheme in which the ciphertext policy is matrix access policy based on LSSS matrix access structure. In 2014, Chung et al. [10] analyzed these CP-ABPRE schemes [6] and made comparisons of them by some criteria. In 2015, Kawai [12] proposed a flexible CP-ABPRE scheme in which the re-encryption key generation can be outsourced in Attribute-Based Encryption and proved their scheme is secure in the selective security model.

## 2. PRELIMINARIES

In this section, we define the notations used in this paper and review some cryptographic background.

### 2.1 Notations

The notations used in this paper are listed in Table 1.

**Table -1:** The Notations used in this Paper

| Notations used in this paper | |
|---|---|
| Acronym | Description |
| AA | Attribute Authority |
| DO | Data Owner |
| SS | Storage Server ( cloud service provider) |
| UG | User Group |
| PRE | Proxy Re-encryption |

### 2.2 Cryptographic Background

In this paper, we use the bilinear pairings on elliptic curves. We now give a brief review on the property of pairing and the candidate hard problem that will be used.

**Definition (Bilinear Map):** A bilinear map is a function combining elements of two vector spaces to yield an element of a third vector space, and is linear in each of its arguments. Matrix multiplication is an example.
Let $G \times G \rightarrow GT$, where G is a Gap Diffie-Hellman (GDH) group and GT is another multiplicative cyclic group of prime order p with the following properties:

(i) Computable: there exists and efficiently computable algorithm for computing e;
(ii) Bilinear: for all h1, h2 $\in$ G and a, b $\in$ Zp, e(ha1, hb2) = e(h1, h2)ab;

(iii) Non-degenerate: e ($g_1$, $g_2$) ≠ 1, where $g_1$ and $g_2$ is a generator of G.

In this system we used the Decisional Bilinear Diffie-Hellman (DBDH) assumption for security proofs proved.

## 3. SYSTEM MODEL AND SECURITY ALGORITHM DEFINITIONS

In this section we provide the construction of our system model and security algorithm definitions for a ciphertext policy attribute-based Proxy Re-encryption scheme (CP_ABPRE).

### 3.1 System Model

We present the system model for CP_ABPRE scheme in Fig. 1 Compared with the model for typical CP-ABE, Access control policy and Proxy re-encryption scheme are additionally involved.

The various system models for CP_ABPRE scheme are following:

Attribute Authority: Authority will have to provide the key, as per the user's key request. Every users request will have to be raised to authority to get access key on mail.

Data owner: Data owner will have to register initially to get access to the profile. Data Owner will upload the file to the cloud server in the encrypted format. Random encryption key generation is happening while uploading the file to the cloud. Encrypted file will be stored on the cloud.

User group (Consumer): Data consumer will initially ask for the key to the Authority to verify and decrypt the file in the cloud. Data consumer can access the file based on the key received from mail id. As per the key received the consumer can verify and decrypt the data from the cloud.

Cloud Storage Server: Cloud server will have the access to files which are uploaded by the data owner. Cloud server needs to decrypt the files available under their permission. Furthermore data user will have to decrypt the data to access the original text by providing the respective key. File has been decrypted successfully and provided for consumer

Proxy Re-encryption: Receive all ciphertext from the data owner's uploaded file and store all ciphertext. Used the proxy server to re-encrypt this ciphertext and store this re-encrypted file and send this file to data owner provides credential of particular user.

### 3.2 Security Algorithm Definitions

In this system model, we provide algorithm definitions as following:

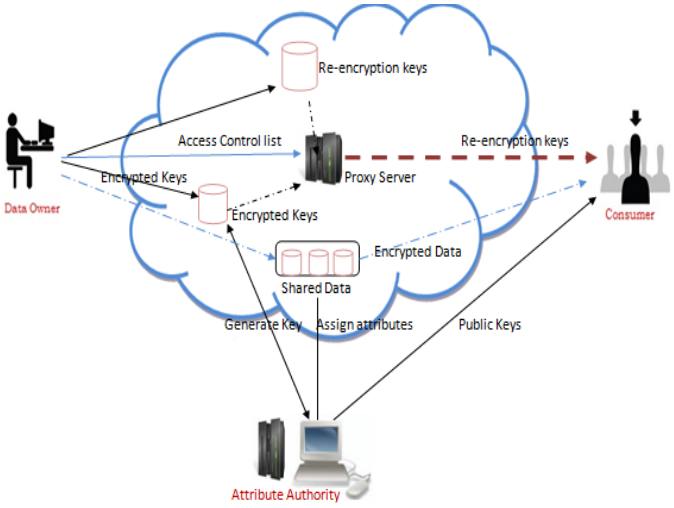


**Fig -1**: System model for CP_ABPRE scheme

**Setup** ($\lambda^{\kappa}$): The setup algorithm calls the group generator algorithm G($\lambda^{\kappa}$)[23] and obtains the descriptions of the two groups and the bilinear map $D$ = ($p$;G0;G1; $g$; $e$), in which $p$ is the prime order of the cyclic groups G0 and G1, $g$ is a generator of G0 and $e$ is a bilinear map. The Attribute authority (AA) generates the universe of system attributes S = ($att1$, $att2$,..., $attn$) where $n$ is a positive integer. AA has select the randomly attribute and this algorithm produce outputs the Public Parameters (PP) and Master Secret key (MS).

**KeyGen**(MS,L): Let L = [L1, L2, · · · , Ln] be the attribute list for the user who obtains the corresponding secret key. This algorithm generates the Output of secret key (SKL).

**PriKeyGen**(MS, S): The Private Key (PK) Generation algorithm is run by the attribute authority. It takes as inputs the Master secret MS and the attribute set of user S. It outputs the private key of user (PK) Private Key associated with the attribute set of user S.

**Encrypt** (PP, A1, A2, PK): The Encryption Key Generation algorithm is run by the delegator. It takes as inputs the public parameters PP, the access structures A1 and A2, and the private key PK. It outputs a unidirectional re-encryption key RKA1->A2 which is employed by the proxy to re-encrypt the original cihpertext CT

**ReEncrypt**(PP,CT,RKA1->A2): The Re-Encryption algorithm is run by the proxy. It takes as inputs the public parameters PP, the ciphertext CT and the re-encryption key RKA1->A2. It outputs the re-encrypted ciphertext CT' associated with the access structure.

**Decrypt** (CT', PK) : The Decryption algorithm is run by the User who is request the particular file to decrypt . It takes as inputs the CT' and the private key PK. [22]It outputs the plaintext message M if attribute set S satisfies the access structures $A_k$ (k = 1, 2), else it returns NULL.

## 4. PERFORMANCE ANALYSIS

Our proposed system solves the problem of security of documents while uploading implementing a secure and efficient access control mechanism across cloud platform with N users. For performance measure we compare the computational overhead that is incorporated in implementing secure proxy re-encryption and access control mechanism. Computational overhead is involved in process of proxy re-encryption which is measured in terms of time cost required to generate N tags for document D uploaded by N users. As document length increases the number of blocks increases which incurs more tags to be created thus increasing the time required for generating tags.

The proposed system is implemented in Java. The web services are hosted in Apache Tomcat 7. At front end, JSP has used. Coding of application is done with JDK 1.7.Here MYSQL 5 database is used as back end for storing data and NetBeans IDE 7.2.1 is used as IDE with INTEL 2.8 GHz i3 processor and 4 GB RAM with Jelastic cloud service provider are used to deploy the code within the cloud. The Proposed System divided into Five modules: User, Cloud Service Provider, Attribute Authority and Proxy Re-encryption are perform.

**Table -2: System performance**

| File Size(in KB) | File Encryption time (in ms) | File Decryption time (in ms) |
|---|---|---|
| 10 KB | 515 | 512 |
| 20 KB | 1026 | 1033 |
| 27 KB | 1780 | 1759 |
| 40 KB | 2260 | 2033 |

The above table shows the dual algorithms performance for user plain data conversion as well encryption decryption.
In second experiment Fig.2 shows data encryption performance which works to show that the data it will encrypt in how much time in seconds. Suppose there is a 100kb data is encrypted in 5149msec so the result will display automatically in that time of encryption data from the users.

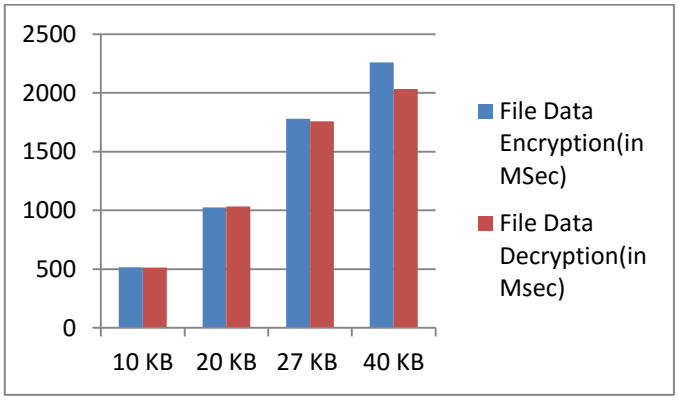


**Fig -2**: Performance analysis of CP_ABPRE scheme base on data size

## 5. CONCLUSIONS

In this paper, we proposed a new security model of CP-ABPRE scheme, which supports attribute-based dual system encryption technology and selectively secure access control policy. CP-ABPRE employs the PRE technology in the ABE cryptographic setting and could be applicable to many real world applications, such as email forwarding. We proposed a ciphertext policy attribute based proxy re-encryption scheme which delegates the proxy to transform the access structure associated with the original ciphertext without decrypting it

## ACKNOWLEDGEMENT

A very firstly I gladly thanks to my project guide Dr. B. L. Gunjal, for her valuable guidance for implementation of proposed system. I will forever remain a thankful for their excellent as well as polite guidance for preparation of this report. Also I would sincerely like to thank to HOD of computer department Mr. R. L. Paikrao and other staff for their helpful coordination and support in project work

## REFERENCES

1. D. G. Feng and C. Chen, "Research on attribute-based cryptography," *Journal of Cryptologic Research*, vol. 1, no. 1, pp. 1–12, 2014.
2. V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS '06)*, pp. 89–98, Alexandria, Va USA, October 2006.
3. Q. Y. Li andF.L.Zhang, "Afully secure attribute based broadcast encryption scheme," *International Journal of Network Security*,vol. 17, no. 3, pp. 263–271, 2015.

4. K. T. Liang, L.M. Fang,D.S.Wong, andW.Susilo, "A ciphertext policy attribute-based proxy re-encryption scheme for data sharing in public clouds," *Concurrency and Computation: Practiceand Experience*, vol. 27, no. 8, pp. 2004–2027, 2014.
5. C.-C. Chang, C.-Y. Sun, and T.-F. Cheng, "A dependable storage service system in cloud environment," *Security and Communication Networks*, vol. 8, no. 4, pp. 574–588, 2015.
6. X. Liang, Z. Cao, H. Lin, and J. Shao, "Attribute based proxy re-encryption with delegating capabilities," in *Proceedings of the 4th International Symposium on ACM Symposium on Information, Computer and Communications Security (ASIACCS '09),* pp. 276–286, ACM, March 2009.
7. S. Luo, J. Hu, and Z. Chen, "Ciphertext policy attribute-based proxy re-encryption," in *Information and Communications Security*, M. Soriano, S. Qing, and J. L´opez, Eds., vol. 6476 of *Lecture Notes in Computer Science*, pp. 401–415, Springer, Berlin,Germany, 2010.
8. H. Seo and H. Kim, "Attribute-based proxy re-encryption with a constant number of pairing operations," *International Journal of Information and Communication Engineering*, vol. 10, no. 1, pp. 53–60, 2012.
9. K. Y. Li, "Matrix access structure policyused in attribute-based proxy re-encryption," http://arxiv.org/abs/1302.6428.
10. P.-S. Chung, C.-W. Liu, andM.-S. Hwang, "A study of attribute based proxy re-encryption scheme in cloud environments," *International Journal of Network Security*, vol. 16, no. 1, pp. 1–13,2014.
11. K. T. Liang, L. M. Fang, D. S. Wong, and W. Susilo, "A ciphertext-policy attribute-based proxy re-encryption with chosen-ciphertext security," Tech. Rep. 2013/236, IACR Cryptology ePrint Archive, 2013.
12. Y. Kawai, "Outsourcing the re-encryption key generation: flexible ciphertext-policy attribute-based proxy re-encryption," in *Information Security Practice and Experience*, vol. 9065 of *Lecture Notes in Computer Science*, pp. 301–315, Springer, Berlin,Germany, 2015.
13. A. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters," Fully secure functional encryption: attribute-based encryption and (hierarchical) inner product encryption," in *Advances in Cryptology—EUROCRYPT 2010*, H. Gilbert, Ed., vol. 6110 of *Lecture Notes in Computer Science*, pp. 62–91, Springer, Berlin, Germany, 2010.
14. K. Liang, M. H. Au, W. Susilo, D. S. Wong, G. Yang, and Y. Yu, "An adaptively CCA-secure ciphertext-policy attribute-based proxy re-encryption for cloud data sharing," in *Information Security Practice and Experience: 10th International Conference ,ISPEC 2014, Fuzhou, China, May 5–8, 2014. Proceedings*, vol.8434 of *Lecture Notes in Computer Science*, pp. 448–461,Springer, Berlin, Germany, 2014.
15. A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Advances in Cryptology—EUROCRYPT 2005: 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, May 22–26, 2005.*
16. A. Shamir, "Identity-based cryptosystems and signature schemes," in *Proceedings of the Advances in Cryptology (CRYPTO '84)*, pp. 47–53, Springer, Berlin,Germany, 1985.
17. L. J. Pang, J. Yang, and Z. T. Jiang, "A survey of research progress and development tendency of attribute-based encryption," *The Scientific World Journal*, vol. 2014, Article ID 193426, 13 pages, 2014.
18. L. Cheung and C. Newport, "Provably secure ciphertext policy ABE," in *Proceedings of the 14th ACM Conference on Computer and Communications Security (CCS '07)*, pp. 456–465,November 2007.
19. T.Nishide, K. Yoneyama, and K.Ohta, "Attribute-based encryption with partially hidden encryptor-specified access structures," in *Applied Cryptography and Network Security (ACNS 2008)*, pp. 111–129, Springer, Berlin, Germany, 2008.
20. J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *Proceedings of the IEEE Symposium on Security and Privacy (SP '07)*, pp. 321–334, IEEE Computer Society, Berkeley, Calif, USA, May 2007.
21. V. Goyal, A. Jain, O. Pandey, and A. Sahai, "Bounded ciphertext policy attribute-based encryption," in *Proceedings of the International Colloquium Automata, Languages and Programming (ICALP '08)*, pp. 579–591, Springer, Berlin, Germany, 2008.
22. Huixian Li and Liaojun Pang," Efficient and Adaptively Secure Attribute-Based Proxy Reencryption Scheme", Hindawi Publishing Corporation International Journal of Distributed Sensor Networks , Article ID 5235714, pp.1-12,2016
23. Song Luo, Jianbin Hu, and Zhong Chen ,"Ciphertext Policy Attribute-Based Proxy Re-encryption", Springer-Verlag Berlin,, pp. 401–415, 2010.
24. X. H. Liang, Z. F. Cao, H. Lin, and D. S. Xing, "Provably secure and efficient bounded ciphertext policy attribute based encryption," in *Proceedings of the 4th International Symposium on Information, Computer, and Communications Security (ICCS '09)*, pp. 343–352, Sydney, Australia, March 2009..