*International Journal on Applications in Information and Communication Engineering*
*Volume 1: Issue 3: March 2015, pp 61-62. www.aetsjournal.com* ISSN (Online) : 2394-6237

# Secure Data Sharing and Efficient User Revocation for Certificate less Encryption

R.Priya, N.Poongothai

***Abstract—*** A Certificateless public key encryption scheme allows any body to encrypt a message for a particular receiver using publicly available information (in exactly the same way as a traditional public-key encryption scheme or an identity based encryption scheme). However, unlike a traditional public key encryption scheme, no certificates are needed. This is because an attacker who publishes a false public key pk ID for an identity will still not be able to decrypt messages encrypted under that public key, because the key generation centre will not release the partial private key to the attacker and so the attacker will not be able to compute the full private key. We propose a novel approach to securely share data in a public cloud. Unlike conventional approaches, the KGC only needs to be semi-trusted and can reside in the public cloud, because our mCLPKE scheme does not suffer from the key escrow problem and revocation problem.

***Keywords—*** Access control, Certificateless cryptography, confidentiality, Cloud computing.

## I. INTRODUCTION

Due to the emerging trends of public cloud storage, many organizations have migrated to adopt public cloud services like Dropbox and Microsoft Skydrive to manage their data. In order to adopt to these public services, the public storage model must solve data confidentiality issues. That is, the stored data must be shared securely from unauthorized accesses. The most frequently used approach to assure data confidentiality is to encrypt the data before uploading to public storage. Many organizations supports fine grained encryption based access control in which it encrypts different sets of data items to which the same access control policy applies with different symmetric keys and give users either the relevant keys or the ability to derive the keys.

The key derivation approach reduces the number of keys to be managed; symmetric key based mechanisms have the problem of high cost of key management. In order to reduce this overhead an alternative method called public key cryptosystem is used. The public key cryptosystem uses certificate authority to issue digital certificate for each users public key thereby the overall certificate management is very complex and expensive. To address this shortcoming, Identity Based Public Key Cryptosystem (IB-PKC) was introduced, but it suffers from key escrow problem as the key generation center learns the private keys of all the users. Alternatively, Attribute Based Encryption (ABE) was introduced, but it suffers from revocation problem which means that the private keys given to the user should be updated when they revoked. In order to address the key escrow problem certificateless public key cryptosystem was introduced. But they rely on pairing approach. The computational cost required for pairing approach is high when compared to the cost of standard operations such as modular exponentiation in finite fields. Certificateless public key encryption (mCL-PKE) solves the key escrow problem in identity based encryption and certificate revocation problem in public key cryptography.

In this paper we propose a novel mediated Certificateless Public Key Encryption (mCLPKE) scheme that does not use pairing operations and assure the confidentiality of data stored in public clouds by specifying the access control policies. This scheme reduces the computational cost by using a pairing free approach. A policy enforcement point called as security mediator is used to partially decrypt the encrypted data before users decrypt. The security mediator supports instantaneous revocation. In this approach each user needs to maintain its public/private key pair whereas, in symmetric key systems users need to manage number of keys equals to the number of users. Revocation problem is solved in which the private keys of the users need not be changed.

## II. SYSTEM MODEL

The main goal of mCLPKE approach is to provide data confidentiality in public cloud. According to the access control policy the data owner encrypts the message using the symmetric encryption algorithm and uploads the encrypted data to the cloud. Our System consists of KGC, Security mediator, data owner, data user and the storage service. The main role of KGC is to generate keys thereby it resides on public cloud which simplifies the task of managing keys for organizations. The security mediator is responsible for checking whether the user is revoked when they made data request. In the traditional system the data owner has to encrypt the same data encryption key multiple times for each user using their public keys. In our approach the data owner encrypts the data encryption key only once and provides some additional information to the cloud. The cloud simply acts as a storage service .

Our Scheme consists of the following phases: (1) Cloud server (2) Registration of user (3) Encryption and uploading of data (4) Downloading and decryption of data.

R.Priya, PG Scholar, Department of Computer Science and Engineering, Sasurie Academy of Engineering, Coimbatore. ( Email: priyaktp@gmail.com)
N.Poongothai, Assistant Professor, Department of Computer Science and Engineering, Sasurie Academy of Engineering, Coimbatore.( Email: Poongothai_be@yahoo.co.in)

*A. Cloud server*

The cloud server provides data storage and sharing services to data owners and data users. After verify the member connection under signature, member can able to access the particular owner's data with respect to owner's private key and identity. So the cloud verifies whether the request member is in the revoke list which is send by group manager under signature if so, it provide permission to access the data else throw unauthorized member request. So the revoke list is updated once member leave or join the group by cloud.

*B. Registration of user*

The user generates public/private key pair. Then the user sends its public key and its identity to KGC. The KGC then creates two partial keys and public key for user. One partial key is considered as SEM key, given to security mediator. The other key as KGC key to encrypt the data. The public key is give to user for decryption.

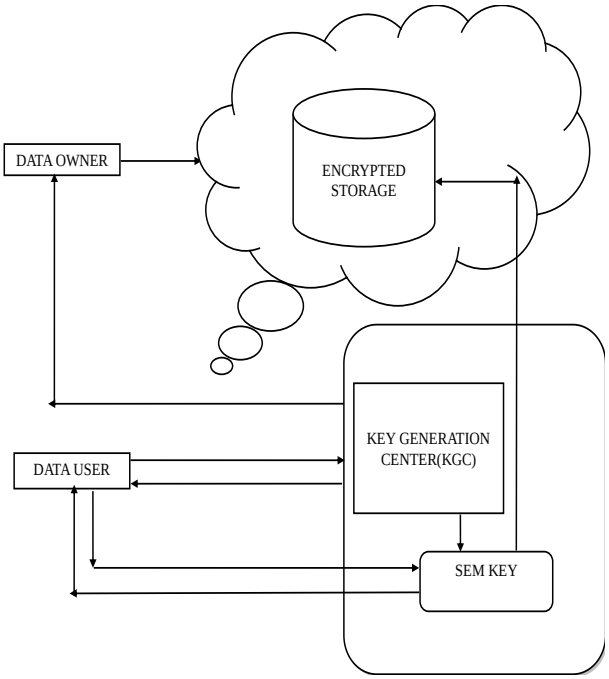
*C. Encryption and uploading of data*

The KGC key which generated is given to data owner for data encryption .The encrypted data along with access control policy is uploaded to the cloud.

*D. Downloading and decryption of data*

The user sends request to the SEM when he wants to read the data. After receiving the request from user the SEM first checks whether the user is revoked or not. If he is revoked then it does not responds to his request. If is not revoked then it partially decrypts the data and perform response for user request thereby making the decryption easier.

The overall system is represented as




## III. CONCLUSION

The first mCL-PKE scheme without pairing operations and provided its formal security. Our mCL-PKE solves the key escrow problem and revocation problem. Using the mCL-PKE scheme as a key building block, we proposed an improved approach to securely share sensitive data in public clouds. Our approach supports immediate revocation and assures the confidentiality of the data stored in an untrusted public cloud while enforcing the access control policies of the data owner. For multiple users satisfying the same access control policies, our approach performs only a single encryption of each data item and reduces the overall overhead at the data owner.

## IV. FUTURE ENHANCMENT

We define the framework for a revocable certificateless signature (RCLS) scheme. It is slightly different from the conventional definition of certificateless signature in a sense that the partial private key is divided into an initial partial private key and a time key. The time key is transmitted to the user via a public channel. The revocation is achieved by stopping the production of new time keys for the revoked user.

## REFERENCES

[1] Al-Riyami.S and Paterson.K, "Certificateless public key cryptography,"in Proc. ASIACRYPT 2003, C.-S. Laih, Ed. Berlin, Germany: Springer, LNCS 2894, pp. 452–473.

[2] Boneh.D, Ding.X, and Tsudik.G, "Fine-grained control of security capabilities," ACM Trans. Internet Technol., vol. 4, no. 1, pp. 60–82, Feb. 2004.

[3] Chow. S. S. M., Boyd. C. and Nieto. J. M. G., "Security mediated certificateless cryptography," in Proc. 9th Int. Conf. Theory Practice PKC, New York, NY, USA, 2006, pp. 508–524.

[4] Goyal V., Pandey O., Sahai A., and Waters.B, "Attribute-based encryption for fine-grained access control of encrypted data," in Proc. 13th ACM Conf. CCS, New York, NY, USA, 2006, pp. 89–98.

[5] Lei Xu X. W. and Zhang X., "CL-PKE: A certificateless proxy reencryption scheme for secure data sharing with public cloud," in ACM Symp. Inform. Comput. Commun. Security, 2012.

[6] Seung-Hyun Seo, Mohamed Nabeel, Xiaoyu Ding, and Elisa Bertino, "An Efficient Certificateless Encryption for Secure Data Sharing in Public Clouds".

[7] Wang S. Yu, C., Ren K., and Lou W.,"Attribute based data sharing with attribute revocation," in Proc. 5th ASIACCS, New York, NY, USA, 2010, pp. 261–270.