ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 2, Issue 12, December 2013

A Two Layer Encryption Approach to Secure Data Sharing in Cloud Computing

Mr. Bhavesh Rahulkar , Mr. Praveen Shende

Abstract— My proposed scheme is 'Two Layer Encryption' means Double Encryption for securely outsourcing the data in cloud. This scheme solves key escrow problem and Data Reveal problem by **RSA algorithm** of **asymmetric key approach**. In existing mCL-PKE scheme there is Certificate-less Encryption and also single encryption and it is half decrypted by the 'CLOUD' and remaining half is decrypted by the 'USER' but in my scheme there will be certification for the User and two layer encryptions. The outer layer encryption will be decrypted by the 'CLOUD' and Inner layer encryption will be fully decrypted by the 'USER' only, By this manner the data/information will be highly secured. My **Aim** is **"To Secure the 'TEXT' Data Items of the Data-Owner by Double Encryption in Cloud Computing"**.

Index Terms—DEA, Decryption center, RSA algorithm, cloud computing, Asymmetric key, Two Layer Encryption.

I. Introduction

Today cloud computing is very popular in IT industry; it supports very large storage to any type of data. Cloud computing is the new technology and it is becoming very essential for the IT industry, Almost all the organizations are adopting this to manage their work efficiently. But there is measure security issue to protect the information in the cloud storage, so there are many techniques to secure the data items, and 'Encryption of the Data' is one of them.

The proposed scheme is "Two Layer Encryption" and it is extended from the previous scheme of mCL-PKE. mCL-PKE scheme works on certificate-less encryption and user is not certified by any authorized entity but in my scheme there will be certification for user, certification of the user also provides security to the information in the cloud, due to this only authorized person can use the data. The **Double Encryption Approach** (**DEA**) means two layer encryption approach addresses the shortcomings of the mCL-PKE scheme. In DEA approach user will have to first register to the owner to get the secret key for decryption of the encrypted documents. The basic scheme is, owner encrypts the documents and sends these encrypted documents to the

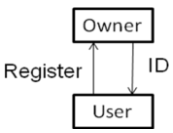

Fig. 1. Certification of the user

cloud, now cloud decrypts the outer-layer of the encrypted contents and sends these documents to the requested users, now user fully decrypts the encrypted contents means inner-layer of the encryption by the secret keys. In this approach there are three main entities (1) Owner, (2) Cloud and (3) User, Cloud has three sub parts that are (1) Encrypted storage,(2) Decryption center, (3) Key Generation Center(KGC).

Encrypted storage stores the documents which are encrypted by the owner, Decryption center partially decrypts the documents, and KGC generates the KGC-key for the owner to encrypt the contents. Cloud is divided into three parts to reduce the time required for all process. Key generation, storage of the encrypted documents and partially decryption of the encrypted documents reduce the total time of the whole process. There are two types of encryption approach or method, (1) Symmetric key, (2) Asymmetric key.

Key is used to encrypt and decrypt the documents, in symmetric key approach the same key is used to encrypt and decrypt the documents but in asymmetric key approach two different keys are used to encrypt and decrypt the documents. In symmetric key approach single/one key is used but two keys are used in asymmetric key approach. Symmetric key technique is faster than asymmetric key technique in encryption and decryption of the documents/information. But asymmetric key technique is better than symmetric key in other behavior.

The key management is easy in asymmetric key technique but in symmetric key it is quite tedious, and key distribution is also easy in asymmetric key technique as compare to symmetric key approach. To provide high security to the data I will use the asymmetric key technique in my system because the security is high in asymmetric key technique as compare to symmetric key technique. In my scheme there is the certification of the users, and asymmetric key approach will be easy and efficient because of its efficient key management. Revocation of the compromised users is very necessary to protect the data from malicious use, hence in my system 'Decryption Center' supports the revocation of the malicious users. In symmetric key system private key of the users have to update but in my system of asymmetric key there is no need of the private key to be changed.

The important thing is that, if more than one user are authorized and they want to access the same document then encryption cost will be very high for data owner because owner has to encrypt the same document multiple times for many users using the user's public key in previous mCL-PKE scheme. To overcome this drawback the extended mCL-PKE scheme is, data owner encrypts the documents only once and provides the additional information to the cloud for authorized users to decrypt the documents.

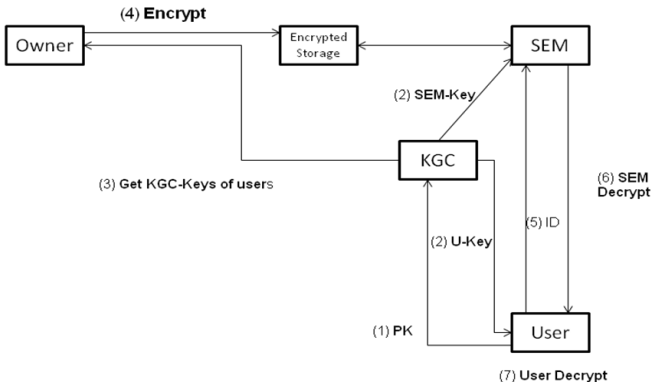

Fig. 2. The basic mCL-PKE scheme

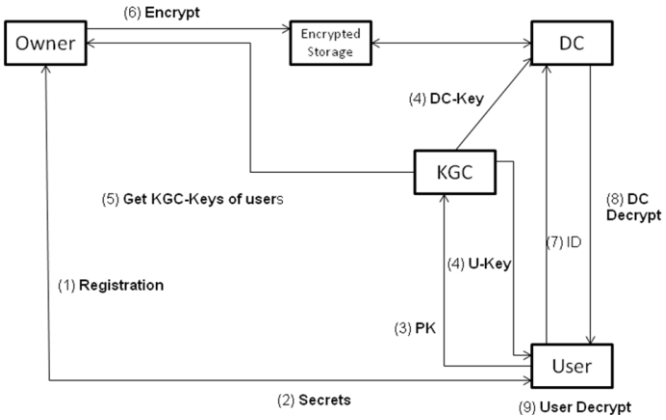

Fig. 3. Improved proposed scheme

II. Related Existing Scheme

Cryptography is the art and science of achieving security by encrypting/encoding data to make them non-readable, the process of encoding plain text messages into cipher text messages is called as **Encryption**, there are many techniques to encrypt the data. Encryption of the data is the method to protect the data from malicious and unauthorized users, encryption of the documents can be more than one layer, many layer of the encryption enhance the security of the content but increase the encryption cost for the owner. The previous certificate-less encryption scheme (mCL-PKE) consists of three main entities:

(1) Owner
(2) Cloud
(3) User.

The cloud has three sub parts, Encrypted Content Storage, Key Generation Center (KGC), and Security Mediation Server (SEM). Encrypted Content Storage stores the encrypted documents, Key Generation Center generates the KGC-key for encryption and Security Mediation Server partially decrypts the encrypted documents.

The BGKM (Broadcast Group Key Management) scheme is proposed by the Mohamed Nabeel and Elisa Bertino, the advantage of this scheme is that adding or revoking users or updating access control policies can be performed efficiently by updating only some public information.

III. Proposed Scheme

In this paper the proposed scheme architecture is divided into three main parts: (1) Owner, (2) Cloud and (3) User. Cloud is further divided into three sub parts; Encrypted Storage (ES), Decryption Center (DC) and Key Generation Center (KGC).

The basic method is **Double Encryption** of the documents means there is two-layer encryption of the data or information. I extend the previous mCL-PKE scheme but in my system there is certification of the users. My simple scheme is owner will encrypt the contents two times using the KGC generated key and stores the documents to the Encrypted Storage, when user request any document the decryption center fetches the requested document and decrypts the outer layer of encryption and gives to the user, now user fully decrypts the document.

In this paper the **RSA algorithm** is proposed which supports asymmetric key approach, RSA algorithm is very easy to implement and enhances the security of the data, and In RSA algorithm malicious users cannot learn the keys.

IV. Expected Results

In this section I propose the basic mCL-PKE scheme then my improved scheme, the basic public key encryption is certificate-less scheme, in which user's certification is not necessary which reduces the management cost. But this scheme compromises to the malicious users, any malicious user can access the data for malicious use. The shortcomings of this scheme is addressed by the improved scheme in my system, in which user must have to register to the owner then only he/she is able to access the information. So this ideology enhances the security of the data.

The basic mCL-PKE scheme propose the single encryption and half decrypted by the cloud and remaining half is decrypted by the user, this scheme is proposed to reduce the decryption time of the user, but partially decryption of the data reduce the security of the content, but in my scheme there is double encryption of the data, there is two layer of the encryption, in which outer layer encryption is decrypted by the cloud and inner layer encryption is decrypted by the user, hence security is high in my improved scheme. The overall result comes that security is very high in my system as compare to previous mCL-PKE scheme.

V. Conclusion

The scheme of double encryption and certification of the users provide high security to the data, and asymmetric key approach (RSA) is very easy in key distribution. The future enhancement of this scheme is that RSA can also be used for performing digital signature and it will be helpful for improving the security in future.

VI. References

[1]. Mohamed Nabeel, Elisa Bertino, Seung-Hyun Seo, Xiaoyu Ding Members of IEEE "An Efficient Certificate-less Encryption for Secure Data Sharing in Public Clouds" June 2013.
[2]. Zhiguo Wan, Jun'e Liu and Robert H. Deng. Senior Member, IEEE "HASBE: A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control in Cloud Computing" April 2012.
[3]. Mohamed Nabeel, Student Member, IEEE, Ning Shang, Elisa Bertino Fellow, IEEE "Privacy Preserving Policy Based Content Sharing in Public Clouds" 2013.
[4]. Mohamed Nabeel, Elisa Bertino Fellow, IEEE "Privacy Preserving Delegated Access Control in Public Clouds" 2013.
[5]. Yang Tang, Patrick P.C. Lee, Member, IEEE, John C.S. Lui, Fellow, IEEE, and Radia Perlman, Fellow, IEEE "Secure Overlay Cloud Storage With Access Control and Assured Deletion" November/December 2012.
[6]. Sushmita Ruj, CSE, Indian Institute of Technology, Indore, India, Milos Stojmenovic, Singidunum University, Belgrade, Serbia, Amiya Nayak, SEECS, University of Ottawa, Canada, "Decentralized Access Control with Anonymous Authentication of Data Stored in Clouds" 2013.
[7]. Smitha Sundareswaran, Anna C. Squicciarini, Member, IEEE, and Dan Lin, "Ensuring Distributed Accountability for Data Sharing in the Cloud" March 2012.
[8]. Junzuo Lai, Robert H. Deng, Chaowen Guan, and Jian Weng "Attribute-Based Encryption with Verifiable Outsourced Decryption" 2013.

First Author

Mr. Bhavesh Rahulkar received the BE (Computer Technology) From RTM Nagpur University, Nagpur (M.H.) in 2008 and pursuit for M.Tech. (Computer Science) From Chhatrapati Shivaji Institute of Technology (CSIT), Durg, Chhattisgarh, India,. He is now attending the Mtech-CS course in CSIT and his research interest include Computer Networks, with Cloud Computing and programming languages (JAVA, PHP, .NET) and Web Development, DBMS.

Second Author

Mr. Praveen Shende, Asst. Prof.,CSE Dept. C.S.I.T. Durg, India, received B.E. (Computer Sc.) in year 2009 and in pursuit for M.Tech. (Computer Sc.) From Chhatrapati Shivaji Institute of Technology (CSIT), Durg, Chhattisgarh, India, His interests are Programming Languages(Java, PHP, Joomla), Cloud Computing and DBMS, Computer Networks, Computer System Architecture.