**Volume 1, Issue 1, November-2015, pp. 1-4**

Macaw International Journal of advanced Research in Computer Science and Engineering (MIJARCSE)

Available online at: http://www.macawpublications.com

# Double Encryption for Securely Outsourcing the Data in Cloud

**Saisree[1] , Kiran [2]**

*SICERT, Ibrahimpatnam,RR Dist.*

**Abstract:-** In this paper we exhibited a novel plan i.e Twofold Encryption for Safely Outsourcing the Information in Distributed computing This plan takes care of key escrow issue and Information Uncover issue by RSA calculation of topsy-turvy key methodology. In existing mCL-PKE plan there is Authentication less Encryption furthermore single encryption. In our proposed plan we have two layer encryption plans by this approach the information/data will be profoundly secured while safeguarding and partaking in cloud environment.

**Keywords—** Double Layer Encryption,RSA algorithm, cloud computing, Asymmetric key,

## I. INTRODUCTION

The proposed scheme is "Double Layer Encryption" furthermore; it is stretched out from the past plan of mCL-PKE. mCL-PKE plan takes a shot at declaration less encryption and client is not affirmed by any approved element but rather in my plan there will be confirmation for client, affirmation of the client additionally gives security to the data in the cloud, because of this just approved individual can utilize the information. The Twofold Encryption Approach (DEA) implies two layer encryption approach addresses the deficiencies of the mCL-PKE plan. In DEA approach client will need to first enlist to the proprietor to get the mystery key for unscrambling of the scrambled records. The essential plan is, proprietor encodes the archives and sends these scrambled reports to the cloud, now cloud decodes the external layer of the scrambled substance and sends these records to the asked for clients, now client completely unscrambles the scrambled substance implies internal layer of the encryption by the mystery keys. In this methodology

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. 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

© 2015, Macaw Publications All Rights Reserved

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.

## II. OBJECTIVE OF THE SYSTEM

Information Security is a noteworthy issue in distributed computing situations. There is such a variety of information security issues connected with distributed computing. Security is a noteworthy issue in any distributed computing, in light of the fact that it is vital to guarantee that just approved access is allowed and secure conduct is normal consequently we proposed RSA calculation of awry key approach this give correspondence security over the Web in this manner keeping up privacy of information.

## III. BACKGROUND

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.

## IV. FRAMEWORK

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).

© 2015, Macaw Publications All Rights Reserved

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.

**RSA**:- Ron Rivest, Adi Shamir and Leonard Adleman described the RSA algorithm in 1978. The letter RSA is abbreviating form by initials of their surname. RSA algorithm involves three steps algorithm key generation, encryption and decryption. In this RSA algorithm, m is known as the modulus, „E" is known as the encryption exponent or public key exponent and „D" is known as the decryption exponent or private key exponent. Algorithm [5]:

1. Choose two large prime P & Q
2. Calculate N = P * Q
3. Select the public key (i.e. encryption key) E such that it is not a factor of (P - 1) and (Q - 1).
4. Select the private key (i.e. decryption key) D such that following equation is true:

(D * E) mod (P - 1) * (Q - 1) = 1

5. For encryption calculate cipher text CT from the plain text PT as follows: CT = PTE mod N
6. Send CT as the cipher text to the receiver.
7. For decryption, calculate the plain text PT from the cipher text CT as fallows: PT = CTD mod N

## V. RESULTS

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.

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,

## VI.CONCLUSION

The plan of double layer encryption and accreditation of the clients give high security to the information, and awry key methodology (RSA) is simple in key circulation. The future upgrade of this plan is that RSA can likewise be utilized for performing advanced mark and it will be useful for enhancing the security in future.

## 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.

© 2015, Macaw Publications All Rights Reserved

[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.
[9] Veerraju Gampala, Srilakshmi Inuganti, Satish Muppidi —Data Security in Cloud Computing with Elliptic Curve Cryptography‖ International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-3, July 2012. [11] N. Koblitz. Elliptic curve cryptosystems. Mathematics of Computation, 48:203–209,1987.
[10] V. Miller. Use of elliptic curves in cryptography. Advances in Cryptology—CRYPTO '85 (LNCS 218) [483], 417– 426, 1986.

© 2015, Macaw Publications All Rights Reserved 