Volume 1, Issue 1, November-2015, pp. 16-20

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

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

Dynamic Group data sharing framework on Cloud Servers

Mallesh Goud [1],Pratika Malya[2]
Department of CSE, SRIT. Anatapuram
JNTU Anatapur, Andhra Pradesh, India

Abstract: - In this paper, we proposed a secured multi-owner data sharing scheme for a dynamic group in people, in general, cloud. By furnishing AES encryption with Convergent key while transferring the information, any cloud client can safely impart information to others. In the meantime, the capacity overhead and encryption calculation expense of the plan are free with the quantity of repudiated clients. Also, I break down the security of this plan with thorough confirmations. One-Time Secret word is one of the simplest and most well-known types of confirmation that can be utilized for securing access to accounts. One-Time Passwords are frequently alluded to as secure and more grounded types of confirmation in a multi-owner manner. Broad security and execution examination demonstrates that our proposed plan is profoundly productive and fulfills the security necessities for open cloud-based secure group sharing.

Keywords: Cloud computing, broadcast encryption.

I. INTRODUCTION

Cloud primarily refers to saving of user's data to an offsite storage system that is maintained by a cloud provider. This means instead of storing information on user computer's hard disk or other storage devices, client save it to a cloud database where internet provides the connection between user computer and the cloud provider database. Cloud computing is the hottest topic of discussion in the IT & research world today. IT world is expecting profound miracles to happen with the intervention of cloud services in all spheres of business. It is a new utility computing model in which resources are pooled to provide everything as a service to many users as possible by sharing the available resources.

Cloud computing is actually a combination of various traditional computing techniques like grid computing ,distributed computing, virtualization , load balancing ,etc. It combines the functionalities of all these and is evolve

As a new model on which everyone can rely for everything.

1. Cloud Service Provider (CSP): It is an entity, which manages Cloud Storage, has significant storage space to preserve the clients' data and high computation power.

2. Owner/Organization: Which has large data files to be stored in the cloud and relies on the cloud for data maintenance and computation; it can either be individual Owner or company.

3. User: It is a unit, which is registered to the owner and uses the data of owner stored in the cloud. The user may be an owner itself. The various security concerns and upcoming challenges are addressed in (Wilson and Daniel), 2003; Dimakakos et al., 2009) and also reviewed in terms of standards such as ITIL, PCI-DSS, and ISO-27001/27002. There are architectural security issues which are changing according to various architectural design functioning over cloud computing. Since outsourcing is the main theme of cloud computing, there are main two concerns in this area: External attacker (any unauthorized person) can attack get to the critical data, user has no control over data

Cloud service provider can breach the owner data is to be kept in his premises.

The proposed method for data security has been framed by bringing together various techniques and utilizing them to perform the task of data security in cloud. The model uses encryption as the main fundamental protection scheme and data sent to cloud is in encrypted data form. Encryption is the conversion of data into encrypted form called a cipher text that cannot be easily understood by unauthorized person and can be decrypted by the authorized person having a valid decryption key. In this computing model, owner sends the encrypted data to cloud where it is stored and then the data can be retrieved from the cloud by user, when they request. However, this details to cloud and then search the data with help of keyword obtained from the owner.

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 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

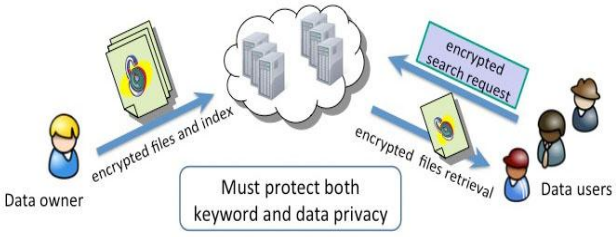

Fig 1. Data privacy in Cloud Computing

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.

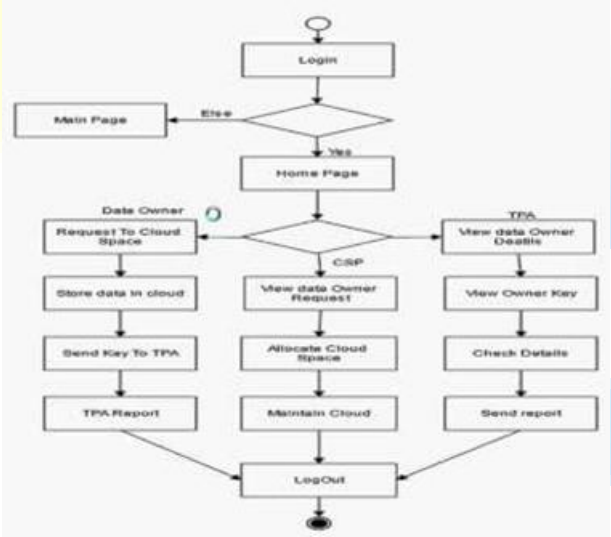

Fig 2. mCL-PKE scheme Activity Diagram

II. PROBLEM STATEMENT

Data Security is a major issue in cloud computing environments. There are so many data security issues associated with cloud computing. Security is a major issue in any cloud computing, because it is essential to ensure that only authorized access is permitted and secure behavior is expected Hence we proposed RSA algorithm of asymmetric key approach this provide communication security over the Internet thus maintaining confidentiality of data.

III. RELATED WORK

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. 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).

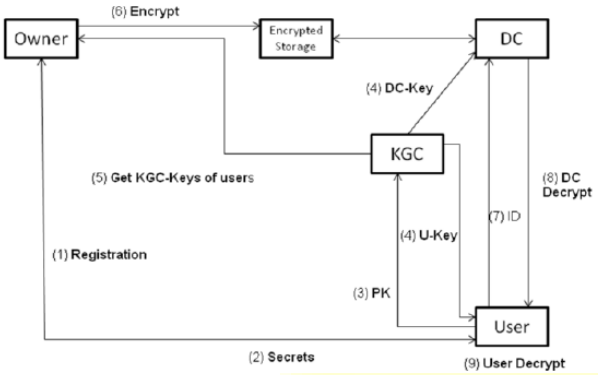

Fig 3. Improved proposed scheme

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

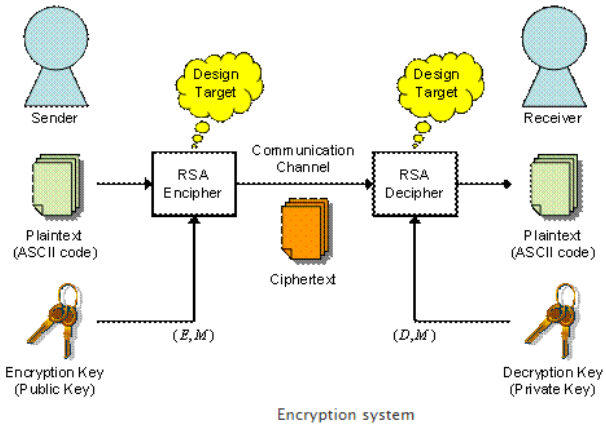

Fig 4 .RSA Public key encryption

V. 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.

VI.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.

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.

[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.