Double Layer Encryption Algorithm Key Cryptography for Secure Data Sharing in Cloud

Dr.D.Usha, M.Subbbulakshmi

Abstract— Cloud technology is extremely beneficial and valuable in present new technological epoch, where a person uses the remote servers and the internet to provide and preserve data as well as applications. Such application in revolve can be used by the users via the cloud infrastructure without any installation. Moreover, the users' data files can be accessed and manipulated from any other computer using the internet services. Despite the flexibility of data and application accessing and usage that cloud computing environments provide, there are many questions still coming up on how to achieve a trusted environment that guard application and data in cloud from unauthorized intruders. Since this paper propose a new era of key cryptography double layer encryption to make the cloud model more secure and trust worthy and a lot of work is being done regarding this. This paper aims to suggest an approach which is a double layer encryption method to ensure security in cloud. It is based on a popular cryptography algorithm RSA which is a relatively novel technique. This scheme resolves key escrow difficulty and data expose problem by RSA algorithm of public key cryptography approach. In this proposed double layers encryption schemes, the data will be extremely secured while protecting and sharing in cloud environment. This scheme not only makes full use of the great processing skill of cloud computing but also can efficiently ensure cloud data privacy and security.

Index Terms— Cloud Storage, Security, Privacy, RSA, Encryption, Cryptography, Double layer encryption.

1 Introduction

Nowadays, the technology has been developed based on the human requirements in the world. Lots of technologies are invented today and each one serves to people in different ways. This technology requires the resources like hardware, software for the effective utilization. From the efficient use it is processed with massive amount of data. The amount of data to handle in this world is completely panic. This situation brings us into a solution cloud computing. Cloud computing is a model for enabling convenient ubiquitous and on demand network access to a common pool of configurable computing resources. Storage of data becomes a main concern in the technical world. The amounts of data are easier to store and maintain with the help of cloud data storage services. It helps to store any large size of the data at different storage positions. Each position is operated in independent way. Business users are also being attracted by cloud storage due to its too many benefits, including lower cost, greater agility, and better resource utilization. However, while enjoying the quality of being useful, easy of distribution data via cloud storage, users are also increasingly worried about inadvertent data leaks in the cloud. Such data seep out caused a malicious. A misbehaving cloud operator, can usually lead to behave badly break or fail to observe of personal privacy or business secrets (e.g., the recent high probe incident of a famous person photos being leaked in iCloud). To address users relate to protect potential data leaks in cloud storage, a prevalent way of dealing with a circumstances is for the data owner to encrypt all the data before upload to cloud. In common privacy refers the condition or state of hiding the presence or view. There is a need to attain this state in the places where the private things are used such as data and files. In cloud data storage the privacy is needed to attain for the data, user identity and on controls. Violation of privacy leads to major failure in the system. To maintain the data privacy, it is possible for a successful deployment and usage of any service. 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. Cryptography is an antique art of hiding data to protect it from malicious users. The information to be sent over the network called plaintext is converted into unreadable form called cipher text by some encryption algorithm. On the receiver's side, the original data can be recovered from the cipher text by applying a decryption algorithm on it. Several algorithms are used to encrypt and decrypt the secret information. These are broadly classified as symmetric and asymmetric methods. Symmetric methods use the similar key for encryption and decryption while asymmetric methods use two keys (private key and public key).

In this paper the main task is to maintain the security and privacy for the data that is uploaded and the challenging problem is to allow only the authorized users to access the data from the cloud. Then the unauthorized users should not be permitted to access the data. In this paper multi-encryption system is proposed to provide the extra security for the data. The double-layer-encryption is performed by the data owner. If the user has to access the data then double-layer decryption should be done so that the safety and privacy of the data is high. The challenging problem is to monitor the attackers. Privacy of the users is taken in to account and only the authorized users are permitted to access or download the data to the cloud. Cloud Admin issues the token and maintains the keys of the users.

2 Literature Survey

1. An Efficient Certificate-less Encryption for Secure Data Sharing in Public Clouds

By Mohamed Nabeel, Elisa Bertino, Seung-Hyun Seo, XiaoyuDing Members of IEEE, June 2013. This paper proposes a certificate-less encryption algorithm for secure data sharing in public clouds.

2. A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control in Cloud Computing
   By Zhiguo Wan, Jun̋e Liu and Robert H. Deng. Senior Member, IEEE, HASBE, April 2012. This paper proposes a Hierarchical attribute based encryption solution for scalable access control in cloud computing.
3. Privacy Preserving Policy Based Content Sharing in Public Clouds
   By Mohamed Nabeel, Student Member, IEEE, Ning Shang, Elisa Bertino Fellow, IEEE, 2013. This paper proposes a policy based content sharing for privacy preserving in public clouds
4. Privacy Preserving Delegated Access Control in Public Clouds
   By Mohamed Nabeel, Elisa Bertino Fellow, IEEE , 2013. This paper proposes a delegated access control algorithm for privacy preserving in public clouds.
5. Secure Overlay Cloud Storage With Access Control and Assured Deletion
   By Yang Tang, Patrick P.C. Lee, Member, IEEE, John C.S. Lui, Fellow, IEEE, and Radia Perlman, Fellow, IEEE, November/December 2012. This paper proposes an efficient access control and assured deletion for secure overlay cloud storage.

3 PROBLEM STATEMENT

Security and privacy of data is the key feature for success of the cloud computing. In several surveys and researches it is stated that privacy is now the major challenge to be deal within cloud. It has presented itself several of the cloud computing security issues which are similar to the traditional ways of in-house computing in new way. This requires re-assessing the risks related to each of the critical areas in new hazardous environment, where the resources are shared by multiple users as discussed. Depending on the cloud model which user use the level of multi-tenancy and security issues would be different. But without any reservation, Infrastructure-as-a-Service (IaaS) of public and private cloud, risks highest amongst all. A number of security managing principles and procedures have been intended to safeguard the cloud storage, but nevertheless its security is at a high risk due to the innovative hacking techniques. Data Security and privacy 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. Cryptography in the cloud employs encryption techniques to secure data that will be stored in the cloud. Hence this paper proposed double layer encryption using RSA algorithm of asymmetric key approach this provide enhanced security over the internet thus maintaining confidentiality of data.

4 DOUBLE LAYER ENCRYTPTION

The implementation of double layer encryption technique is to secure the data of the data-owner by double layer encryption in cloud computing. The basic technique is Double Layer Encryption of the documents means there is two layer encryption of the data or information. The easy technique is data owner will encrypt the data two times using the generated key and upload the data to the cloud Storage. When the user requests any data from the cloud, the authorized user will decrypt the data two times using secrete key and download the data from cloud storage using secrete key. In double encryption technique, the RSA algorithm is one of the best algorithms. On this algorithm use two important keys that secret key and public key, public key is used for encrypting the data in the form of non readable format and secret key is used for decrypting the encrypted data. In the real-world public-key cryptography, RSA algorithm is one of the best algorithms and is widely used to secure data transmission. In RSA, this asymmetric key is used to reduce the real-world difficulty.

The Double Encryption Key Cryptography system is fundamentally design on the basis of key aggregation encryption. Here we are using two keys to encrypt and decrypt the data which are secret key and its aggregate key. The data owner creates the system parameter and constructs a secret key which is public key. Data can be encrypted two times by data owner and he may decide ciphertext associated with the plaintext files which want to be encrypted. The data owner has rights to share the secret key from which can generate an aggregate key which is use for decryption of ciphertext. The decrypt key can be sent to end user through mail id in secure manner. The authenticated user having secret keys can decrypt the file.

This paper consists of five steps which are used to perform the operations. These algorithms implementations having following steps are as follow:

Setup: Data Owner creates an account on the server for sharing of data.

KeyGen: This phase is used for the generation of public key and secret key. The data owner creates a public key to encrypt the data over cloud. It also creates a secret key to decrypt and download the file.

Encrypts and Re-Encrypt: The data owner encrypt and re-encrypt the data by using the public key. This encrypted data is then share among the cloud.

Extract: This phase is used to extract the secret keys for decrypt and download the file from the cloud storage. But other encrypted data remains secure.

Decrypt and Re-Decrypt: The user decrypt and re-decrypt encrypted data using the secret key.

4.1 RSA Algorithm

The RSA algorithm is named after Ron Rivest, Adi Shamir and Len Adleman, who invented it in 1977. The RSA cryptography is the mainly-used public key cryptography algorithm in the world. It can be used to encrypt a message using public key and decrypt a message using secret key without the need to exchange key. The RSA algorithm can be used for both public key encryption and digital signatures. Its security is based on the complexity of factoring huge integers.

Algorithm Steps

The RSA algorithm consists of three steps: key generation, encryption and decryption.

Key Generation

A key is a part of information that determines the efficient output of a cryptographic algorithm. Lacking of key, the algorithm would be worthless. In encryption, a key specifies the particular conversion of plaintext into ciphertext, or vice versa during decryption. There are two keys in RSA, i.e. Public key and Private Key. The public key is known to everyone and is used for encrypting the messages; these messages can be decrypted only using the private key.

- Choose two distinct prime numbers m and n.
- Find t such that $t = p\,q$. t will be used as the modulus for both the public and private keys.
- Find the totient of t, $\phi(t) = (m-1)(n-1)$.
- Choose an e such that $1 < e < \phi(t)$, and such that e and $\phi(t)$ share no divisors other than 1 (e and $\phi(t)$ are relatively prime). e is kept as the public key exponent.
- Determine d (using modular arithmetic) which satisfies the congruence relation
  $de \equiv 1 \pmod{\phi(t)}$.

- The public key is the pair (en, t).
- The private key is the pair (de, t).

Encryption

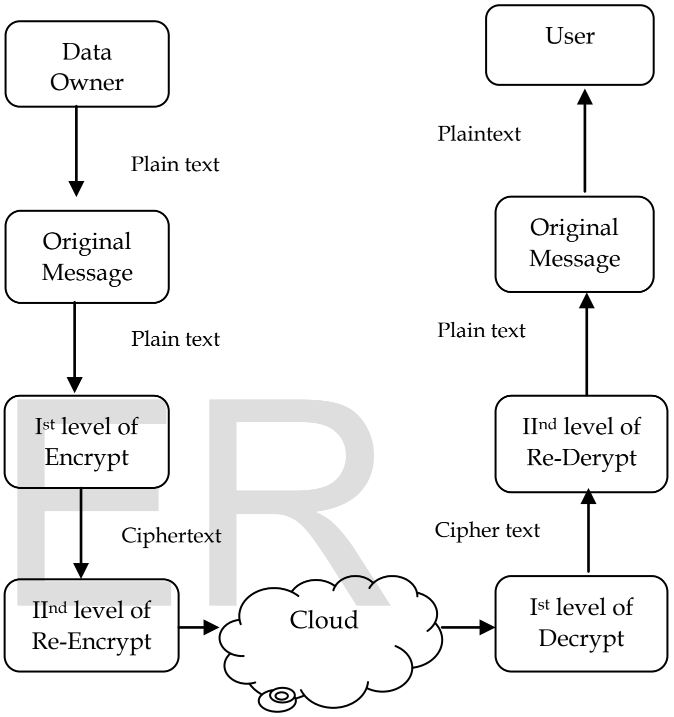
- Data owner transmits his/her public key (modulus n and exponent e) to user, keeping his/her private key secret.
- The data owner, first converts Msg to an integer such that $0 < x < y$ by using agreed upon reversible protocol known as a padding scheme.
- Data owner public key information, the ciphertext ct corresponding to $ct = xe \pmod{y}$.
- Data owner upload message "Msg" in ciphertext, or c, to cloud storage.

Decryption

- User recovers x from ct by using his/her private key exponent, d, by the computation $x = ctd \pmod{y}$.

Given m, user can recover the original message "Msg" by reversing the padding scheme.

4.2 System Model of Double Layer Encryption



4.3 Explanation of System Model

- **Plain Text :** Plaintext means the readable format text (Original Message)
- **Key (Public key) :** The original message is encrypted using public key
- **Encryption Process:** Encryption means the process of converting plaintext into ciphertext. Encryption process contains two level of encryption. In Ist level encryption, the plaintext is converted into ciphertext and IInd level encryption, the ciphertext is converted into ciphertext.
- **Encrypted Ciphertext:** The result of encryption phase (unreadable format).
- **Key (Private Key):** The ciphertext is decrypted using private key.
- **Decryption process:** Decryption means the process of converting ciphertext into plaintext. Decryption process contains two level of decryption. In Ist level decryption, the ciphertext is converted into ciphertext

and IInd level decryption, the ciphertext is conve rted into plaintext.

- **Original Message:** The result of decryption process (Plain Text)

5 Conclusion

In cloud computing, there are different existing techniques that provide security, data confidentiality and access control. Here users need to secure their sensitive information in cloud storage and also to share data with others based on the receiver's ability to manage a policy in distributed systems. The implementation of the double layer encryption technique is going to grant certification for the user to highly secure the data or information. Double Layer Encryption is a good technique to securing the data in the cloud storage. The system is improved to enhance the security model. Thus, sensitive information's are maintained with security and privacy.

References

[1] A. Sahai, J. Bethencourt, and B. Waters, "Cipher text policy attribute-based encryption", in IEEE S& P '07, 2007.

[2] M. Petkovic, S. Nikova, L. Ibraimi, P. Hartel, and W. Jonker, "Ciphertext-policy attribute-based threshold decryption with flexible delegation and revocation of user attributes," 2009.

[3] X. Liang, R. Lu, X. Lin, and X. S. Shen, "Ciphertext policy attribute based encryption with efficient revocation", Technical Report, University of Waterloo, 2010.

[4] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in IEEE INFOCOM'10, 2010.

[5] M. Li, S. Yu, K. Ren, and W. Lou, "Securing personal health records in cloud computing: Patient-centric and fine-grained data access control in multi-owner settings", Sept. 2010.

[6] S. Yu, K. Ren, C. Wang, and W. Lou, "Attribute based data sharing with attribute revocation," in ASIACCS'10, 2010.

[7] https://www.di-mgt.com.au/rsa_alg.html

[8] [8]https://www.tutorialspoint.com/cryptography/public_key_encryption.htm

[9] http://gleamly.com/article/introduction-attribute-based-encryption-abe

[10] https://www.geeksforgeeks.org/rsa-algorithm-cryptography

[11] 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.

[12] Smitha Sundareswaran, Anna C. Squicciarini, Member. IEEE, and Dan Lin, Ensuring Distributed Accountability for Data Sharing in the Cloud, March 2012.

[13] Junzuo Lai, Robert H. Deng, Chaowen Guan, and Jian Weng, Attribute- Based Encryption with Verifiable Outsourced Decryption, 2013.