Design and Analysis of Double Encryption Scheme for Cloud Storage System

S.K. Manigandan*, Sandhiya A, J. Velmurugan and D. Ramya
Dept. of Master of Computer Application, Vel Tech High Tech Dr.Rangarajan Dr.Sakunthala Engineering College, Anna University, Chennai, India.
***Corresponding author: E-Mail: kgmanigandan@gmail.com**

ABSTRACT

A design and analysis of double encryption schema for cloud storage system. The process of encoding a message so that if can be read only by the sender and the intended recipient. To translate the data into a secret code. Encryption is the most effective way to achieve the data security. Encryption systems often use two keys, public key, available to anyone, and a private key that allows only the recipient to decode the message. The receiver needs to occupy dual things in exchange for decrypt the cipher text. The foremost secret key is reserved in the system. The second thing is a particular security device which can be joining up with the system. Without these two things we cannot able to decrypt the cipher text. The Security device is misappropriated this device is revoked. To read an encrypted file, you must have access to a secrete key or password that enables you to decrypt it. Encrypting an email message protects privacy of the message by converting if from plain text into cipher text only the recipient who has the private key that matches the public key used to encrypt the message can decipher the message for reading.

KEY WORDS: Public key, private key, secret key, security device.

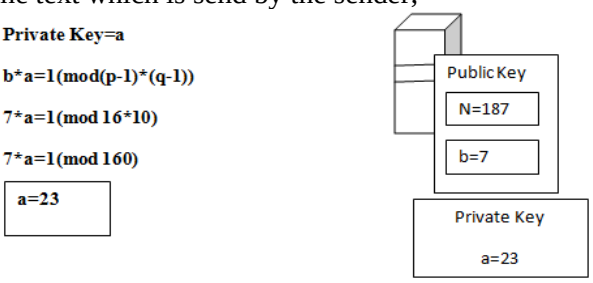
1. INTRODUCTION

A Design and analysis of double encryption schema for cloud storage system. In Existing system it has only one key for the cryptography operation, it uses the same key for encryption and decryption, this key may be stored in the user's Personal computer or in the other local device which can be stored in the device itself it may secured with simple Password, may cause some problem because it may stole, loss or corrupted by any third party systems. If the password is loosed by the user he/she can't able to use the system for encryption/decryption. This is the major issue in the cryptography system to overcome this we use two security mechanisms for secure data Transmission. Cryptographic Primitive is well established low-level cryptographic algorithms that are frequently used to build cryptographic protocols for computer security system. These routine include but are not limited to one way hash function and encrypted function. If the secrete key is leaked up to certain bit. The bit cannot be able to recover the whole secrete key. In Proposed System it proposes a two- factor data security protection mechanisms namely Secret key and secret device .The secret key can be generated with the help of private key generator and the second mechanism is a Unique individual security device.

The user should have the security key and the security device to decrypt the cyber text to the original content. if the user loss/corrupt the security device she/he should Report the SDI (Security Device Issuer) about the device loss, then the SDI issues new Device to the user with the help of this new device the user may continue the process of decryption, After Issues the new device the SDI Should intimate the cloud about the device change . Several of the public key system using in a private key generation. In this system each user has an encryption key that is publicly known and a private key that is known only to that user. The user will encrypt a message with the help of key provided to them. Key generation is the operation of generating keys in the cryptography System. In private key generator it generate the Secret accessing id called private key.

Architecture:

Private key Generator: The private key generator is responsible for providing the Unique Private key for the user while the request to receive or send the data. the private is a unique id for the user which can only known by the user it is secret key for the user to transmit the data .the private key generator is also responsible for generating the private when the user loss their device .this key may be stored in the user's personal device mostly computers. The sender perform two encryption, first the sender encrypt the original text by using the private key and then he/she uses the Security device to re- encrypt the encrypted cipher text, it provide the two security mechanism so the receiver or the user uses two things to decrypt the text which is send by the sender;



Security Device Issuer: Security device is answerable for providing the security device for each user log in to the page. The security device may be a USB, Bluetooth which should be connected to the user's personal computer. The device is responsible for re encrypt the encrypted text. The security device of the user is lost the user request the Security Device Issuer about the device loss, the Security Device Issuer Issues an New Device For the requested User, then the Security Device Issuer Update cloud about the device change, then the cloud may update the cipher text and the cloud may use the new device to encrypt the cipher text. The Security device Issuer is also responsible for storing the data which is transferred between sender and receiver, the SDI Backup the data.

Issuer	**Distributor**	**Applicant**
Set up private/ public key pair		
Package public key with application software	Distribute software	Obtain application
	Distribute hardware	Obtain portable memory device

Sender: The sender is the device or the user who is registered in the website they has unique key called private key and the sender may send the data with the help of security key and the security device. The sender use the Security device to encrypt the data which is send to the receiver and the in the cloud it uses both security key and security device in the cloud it also store the copy of the sending data. The sender only knows the identity of the receiver not more than that using the id the sender sends the data to the receiver. The sender sends the data to the cloud and makes the receiver to download the information from the cloud by using their id.

Receiver: The Receiver is the user who has unique identity; this is used to identify the receiver while sending the data to the receiver. The receiver may use both the secret key and secret device. The secret key may store in the receivers personal computer. The security device contains some secret information which is necessary to decrypt the text in the cloud storage. The private key generator is responsible for providing secret key and security device.

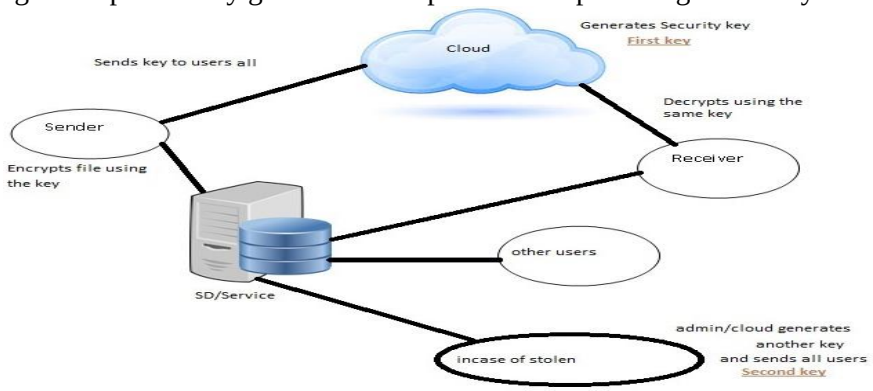


Figure.1. Architecture Diagram

2. MATERIAL AND METHOD

Algorithm: Before the data is encrypted, Key generation should be done. This process is done between the Cloud service provider and the user.

Input: The security device will generate a secret key based on that key, the encryption is formed.

Output:

Step.1. Opt for 2 distinct prime numbers a and b. For security functions, the integers a and b ought to be chosen arbitrarily and will be of comparable bit length.

Step.2. figure n = a * b.

Step.3. figure Euler's totient operate, Ø(n) = (a-1) * (b-1).

Step.4. selected associate number e, specified one < e < Ø(n) and greatest factor of e, Ø(n) is currently e is discharged as Public-Key exponent.

Step.5. currently confirm d as follows: d = e-1(mod Ø(n)) i.e., d is multiplicate inverse of e mod Ø(n).

Step.6. d is unbroken as Private-Key element, so d * e = one mod Ø(n).

Step.7. The Public-Key consists of modulus n and therefore the public exponent e i.e, (e, n).

Step.8. The Private-Key consists of modulus n and therefore the personal exponent d, that should be unbroken secret i.e, (d, n).

3. RESULT AND DISCUSSION

Generating private key using RSA Algorithm: The private key is secret information of the transmission process this key is utilized to encrypt the information which is sent to the receiver over the cloud storage. In a subsisting system, the cloud is utilized to Store the information and additionally used to Encrypt or Decrypt the information for data transmission. This may cause some quandaries like it may slow the haste and the performance of the system. The RSA algorithm stands for Ron Rivets, Aid Shamir, and Leonard Adelman, it publicly described in 1978. It is a Public Cryptography System used for a security purpose. This algorithm is used to prove a secure way to transmit

information's in other words it provide secure communication between the sender and receiver, and it helps the user to secure the sensitive data while transferring the information.

The RSA Algorithm is an Asymmetric cryptography System designates that there are two different keys. This is additionally called public key cryptography, because one of them can be given to everyone. And another one is kept as secret. The public key is kindred to Email Id of the utilize and the private key is akin to Password for the user's email dither public key is kenned by other users in the system or network which avail other users to send the information to the concrete utilize. The password is only ken by the particular utilize to access the secret information.

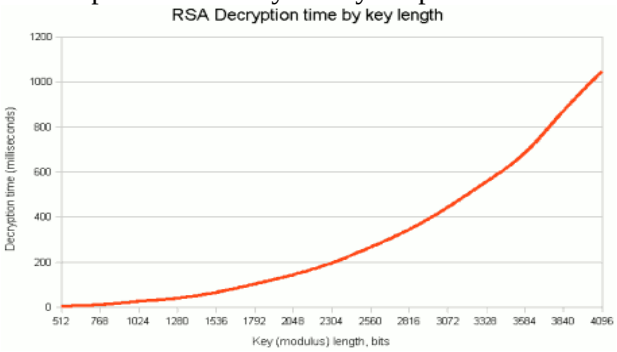


Figure.2. RSA Algorithm analysis

RSA Algorithm Example:

Choose p=5 and q=13

Compute n=p*q=5*13=65

Compute φ (n) = (p-1)*(q-1) =4*12=48

Select such that 1<e<φ (n) and e and n are coprime. Let e=9

Compute a value for d such that (d*e) %φ (n) =1.One solution is d=5[(5*9) %48=1]

Public key is (e, n) => (9, 65)

Private Key is (d, n) => (5, 65)

The encryption of m=2 is $c=2^9$ %65=8

The decryption of c=29 is $m=29^5$%65=51

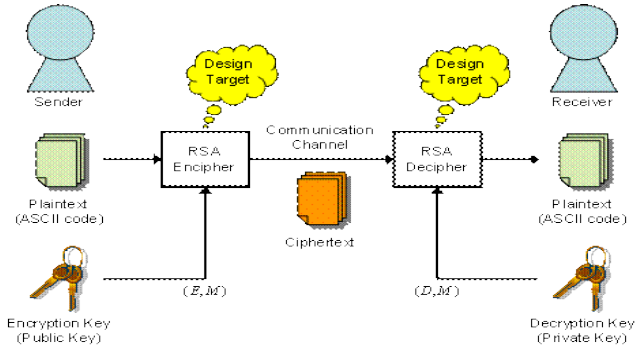


Figure.3. RSA example

Update cipher text after issuing an incipient security contrivance: The Security device issuer issues a secret device to each user in the communication system; the user may use the security device to hold the secure data or information which is used to provide the secure communication in the network.

Each user may contain both the security device and secret Key (private key), if the user loss the security device the user may report the Security Device Issuer about the loss of the security device. Then the SDI issues a new device to a user then the SDI Update the device loss to the cloud to update the cipher text in the cloud and update the key and device of the user in the cipher text. Finally, the user may use the new security device and key to download the cipher text in the cloud and it also uses these security features to decrypt the cipher text to plain text.

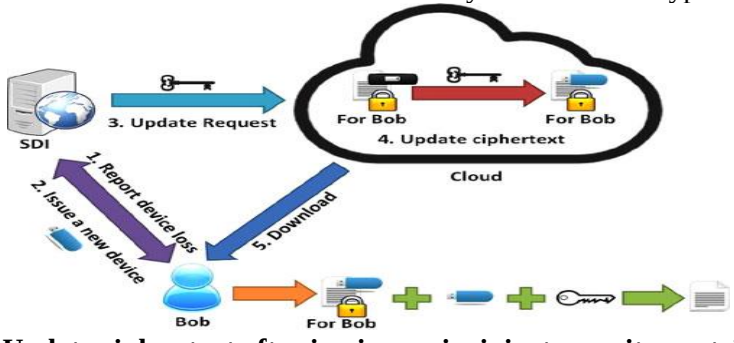


Fig.4. Update cipher text after issuing an incipient security contrivance

Cryptography System: Public-Key cryptography is also known as Asymmetric-Key Cryptography, to differentiate it from the Symmetric-key Cryptography, it uses two keys for Encryption and decryption and these keys are known as Public key and Private Key. With this cryptography system, all users interested in Secure Communication issues their public key.

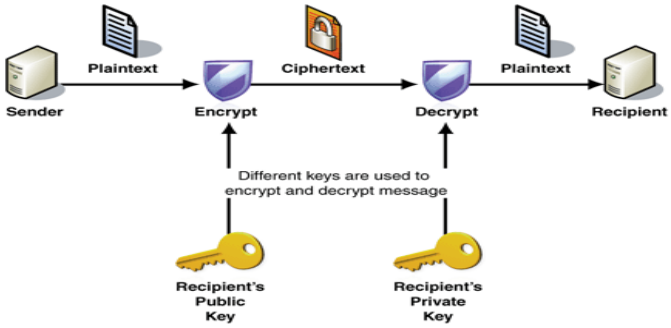


Figure.5. Cryptosystem

User A, if A wants to communicate secretly with User B, can encrypt a message using B's publicly available Key. Such a Communication would only be decipherable by B as only B would have access to the corresponding private key.

User A, if wanting to send an authenticated message to User B, Would encrypt the message with A's Own private key.

Since this message would only be decipherable with A's public key, that would establish the authenticity of the message-means that A was indeed the source of the message.

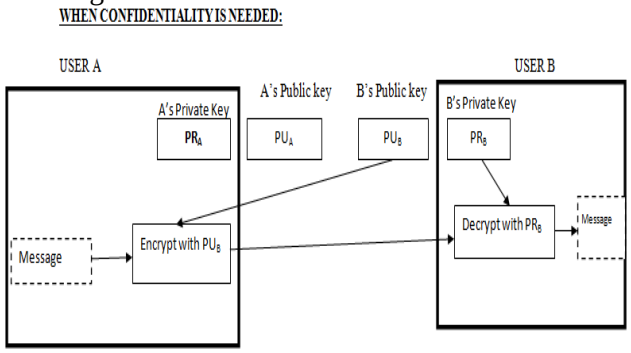


Fig.6. Confidentiality

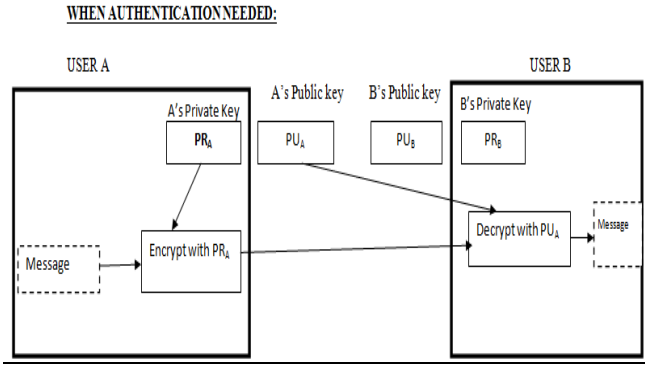


Fig.7. Authentication

Public key Encryption can be used to provide both Confidentiality and authentication at the same time. Confidentiality means that we want to Protect a message from eavesdroppers and authentication means that the recipient needs a guarantee as to the identity of the sender.

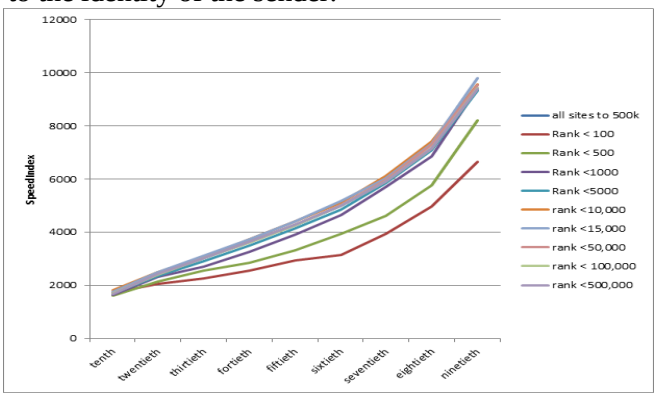


Fig.8. Confidentiality and Authentication

4. CONCLUSION

In this paper, we discussed about the problem in the cryptography system and the security problem in the cloud storage, in existing system the cloud is responsible for storage and cryptography function, it may cause problems like lack of speed and security of information. We propose a new scheme to avoid the problems in the existing system by using another storage device also called Service. In proposed system the storage function can be done by the cloud and the encryption and decryption operation can be done with the help of Service. It may avoid the traffic in the cloud while data transmission. It uses two features for the secure data transmission.

5. ACKNOWLEDGEMENT

The author wish to thank Vel Shree Dr. R. Rangarajan, Chancellor, Vel Tech High Tech Dr. RR and Dr. SR Engineering College, for the support and facilities provided for the preparation of this paper.

Financial disclosure: No financial support was received for this implementation.

REFERENCES

Ashish K, Doolan D, Grandt D, Scott T, and Bates D.W, The use of health information technology in seven nations, Int. J. Med. Informat, 77 (12), 2008, 848–854.

Ashish K, Meaningful use of electronic health records the road ahead, JAMA, 304 (10), 2010, 1709–1710.

Benson T, Principles of Health Interoperability HL7 and SNOMED, New York, NY, USA, Springer, 2009.

Dolin R.H, Alschuler L, Beebe C, Biron P.V, Boyer S.L, Essin D, Kimber E, Lincoln T, and Mattison J.E, The HL7 Clinical Document Architecture, J. Am. Med. Inform. Assoc., 8, 2001, 552–569.

Dolin R.H, Alschuler L, Boyer S, Beebe C, Behlen F.M, Biron P.V, and Shabo A, The HL7 Clinical Document Architecture, J. Am. Med. Inform. Assoc., 13 (1), 2006, 30–39.

Eichelberg M, Aden T, Riesmeier J, Dogac A, and Laleci, A survey and analysis of electronic healthcare record standards, ACM Compute. Sur., 37 (4), 2005, 277–315.

Huang K, Hsieh S, Chang Y, Lai F, Hsieh S, and Lee H, Application of portable CDA for secure clinical-document exchange, J. Med. Syst., 34 (4), 2010, 531–539.

Kuperman G.J, Blair J.S, Franck R.A, Devaraj S, and Low A.F, Developing data content specifications for the nationwide health information network trial implementations, J. Am. Med. Inform. Assoc, 17 (1), 2010, 6–12.

Kwan Y, International standards for building electronic health record (her), in Proc. Enterprise Newt. Compute. Healthcare Ind., 2005, 18–23.

Leahteenmeaki J, Leppeanen J, and Kaijanranta H, Interoperability of personal health records, in Proc. IEEE 31st Annu. Int. Conf. Eng. Med. Biol. Soc., 2009, 1726–1729.

Martınez-Costa C, Menarguez-Tortosa M, and Tomas Fernan- dez-Breis J, An approach for the semantic interoperability of ISO EN 13606 and Open EHR archetypes, J. Biomed. Inform, 43 (5), 2010, 736–746.

Santos MR, Bax MP, and Kalra D, Building a logical EHR architecture based on ISO 13606 standard and semantic web technologies, Studies Health Technol. Informat, 160, 2010, 161– 165.

Yong H, Jinqiu G, and Ohta Y, A prototype model using clinical document architecture (CDA) with a Japanese local standard: designing and implementing a referral letter system, Acta Med the clinical document architecture (CDA), Int. J. Med. Inform., 74, 2005, 245–256.