SECURED DATA SHARING FROM ANONYMOUS USER IN CLOUD STORAGE

Brindhiya J[1], Madhana S[2], Arun K[3]

[1,2]UG Students, Department of CSE, JEPPIAAR SRR Engineering College

[3]Assistant Professor, Department of CSE, JEPPIAAR SRR Engineering College

ABSTRACT: A data can be shared in a secured way from any anonymous user using RSA algorithm. Our system allows a sender to send the data to a receiver through a cloud storage server.User level encryption and decryption is done by AES algorithm. Second level encryption and decryption is done in service provider by RSA algorithm. Once the service provider is hacked, the data are immediately secured by executing the RSA algorithm and stored incloud.

Keywords: RSA,AES,encryption,decryption, cipher text, plaintext.

1. INTRODUCTION

The data in the networked storage system stored in the pool of storage called cloud storage by the third parties. Data accessibility is the notable benefit to use cloud storage system. By the help of network access the data stored in the cloud can be accessed at any time and any place additional storage capacity in storage Maritain task can be offloaded for the responsibility of service provider. Sharing of data between the users is the advantage of cloud storage. The main disadvantage is the out sourcing data increases the attack at the same time same surface area. The possibility of other authorized user to access the data is highly possibly by sharing storage and network with many users. Encryption technologist is a promising solution is deployed to offset the risk the data which is transmitted to and from cloud is protected by encryption technology the data stored in the service provider is also protected as the data as been encrypted, even the unauthorized advisory who as gained accessed to cloud can not get any information about the plain text. Public information are only used by encrypt-er to generate the cipher text whereas the receiver uses secret key to decrypt with the help of encryption algorithm.

2. LITERATUREREVIEW

[1]They proposed two-factor data security protection mechanism with factor revocability for cloud storage system. The sender only needs to know the identity of the receiver but no other information and for decrypt the cipher text the receiver needs to feature two things. The first thing is his/her secret key stored in the computer. The second thing is our computer connects unique personal security device. It is impossible to decrypt the cipher text without either piece. More importantly,the device can be revoked once the security device is stolen or lost. It cannot be used to decrypt any cipher text. This can be done by the cloud server which will instantly execute some algorithms to change the existing cipher text to be un-decry table by this device. This process is entirely transparent to the sender. Moreover, the cloud server cannot decrypt any cipher text at any time.[2]They designed the users should be able to just use the cloud storage as if it localized, without distressing about the need to verify its integrity. Thus, a third party auditor (TPA) is used for cloud storage to check the wholeness of document data and be worry-free. To securely introduce an effective TPA, the auditing process should not bring in new vulnerabilities towards user data privacy, and introduce no additional online burden to user. We further extend our result to enable the TPA to perform audits for multiple users simultaneously and with efficiency. Here, Extensive security and performance analysis are secure and highly efficient.[3]They provides an insightful analysis of the existing status on cloud computing security problems based on a detailed survey carried by theauthor. In cloud computing It alsomakesanattempt to describe the security challenges in Software as a Service (SaaS) model and also endeavors to provide future security research directions.

3.RELATEDWORK

The sender sends the data to receiver only knowing the identity of the receiver.The data is send in an encrypted format to the receiver. This encryption is done by IBE based mechanism.The cipher text is stored in cloud which can be downloaded by the receiver.The decryption depends upon two things one is user's secret key and other is unique personal security device.This security device is uniquely connected to his/ her computer.Without this two things decryption cannot be done.If the security device is stolen or lost,it can be revoked.The cloud will execute another encryption algorithm to encrypt the existing cipher text in that device.The user needs to replace the stolen device so that the cipher text can be regained.This process is completely done at the back end of the sender.

In IBE, the central authority has a key pair which computes the private key corresponding to a given public key. It does not help to recover the whole secret key. The trivial way is to copy the same bits to the new device by the private key generator.The victim user's data can be collected by the adversary by breaking into the computer where the other part of secret key is stored. It has the power to read all files.

4.IMPLEMENTATION

In this proposed system, the security enhancement is done whereas sharing the data between users. To secure the data, two times encryption and decryption isdone.

Techniques used whereas securing data:

- ❖ RNG
- ❖ AES
- ❖ RSA

RNG:

It is abbreviated as Random Number Generation. It is the generation of a sequence of numbers or symbols. It is reasonably unexpected.

AES:

It is abbreviated as Advanced Encryption Standard. Its structure is based on substitution-permutation network. It is symmetric encryption algorithm. It consists of four main function.They are substitute bytes, shift rows, mix columns, add round key.

ALGORITHM:

Step 1: Derive the set of round keys from cipher key.

Step 2: Initialize the state array with block data. (Plain text)

Step 3: Add the initial round key to the starting state array.

Step 4: Perform nine rounds of state manipulation.

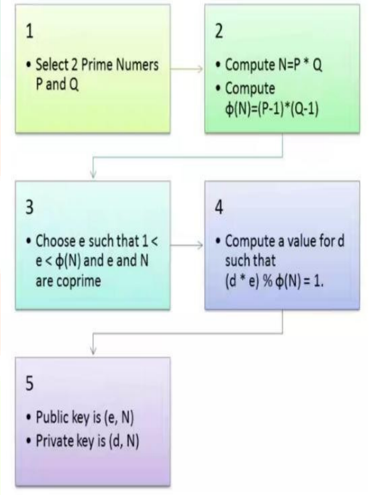
Step 5: Perform the tenth and final round of state manipulation.

Step 6: Copy the final state array as the encrypted data.

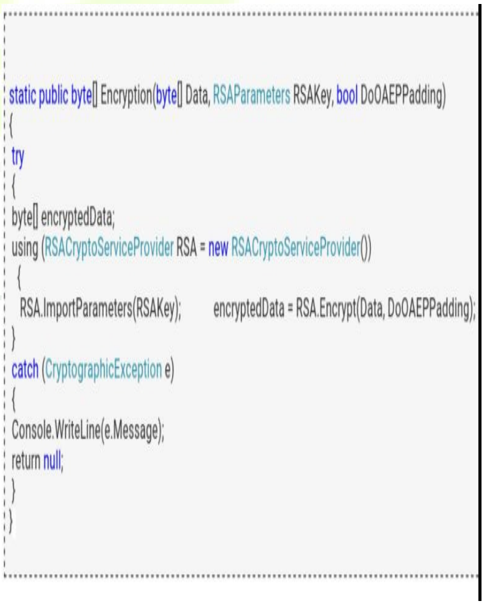
RSA:

It is abbreviated as Rivest Shamir Adleman. It is one of the public key cryptosystem. It is widely used for secured data transmission. A key pair is used for encryption and decryption such as public and private key respectively.It involves four steps: key generation, key distribution, encryption and decryption.

GENERATION OF PUBLIC KEY AND PRIVATE KEY IN RSA:

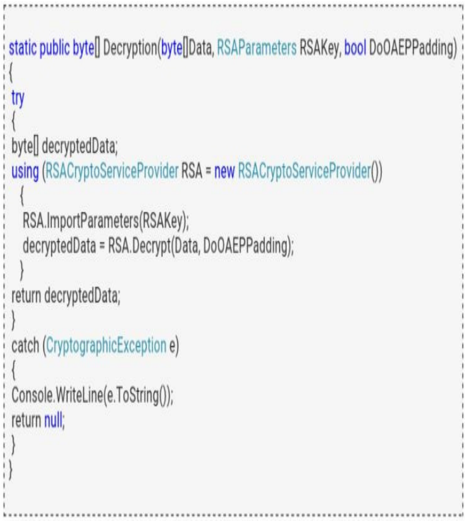

1
• Select 2 Prime Numers P and Q
2
• Compute N=P * Q
• Compute ϕ(N)=(P-1)*(Q-1)
3
• Choose e such that 1 < e < ϕ(N) and e and N are coprime
4
• Compute a value for d such that (d * e) % ϕ(N) = 1.
5
• Public key is (e, N)
• Private key is (d, N)

FUNCTION FOR ENCRYPTION:



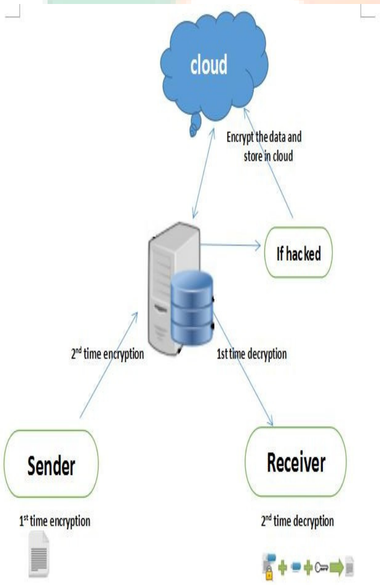
```
static public byte[] Encryption(byte[] Data, RSAParameters RSAKey, bool DoOAEPPadding)
{
try
{
byte[] encryptedData;
using (RSACryptoServiceProvider RSA = new RSACryptoServiceProvider())
 {
  RSA.ImportParameters(RSAKey);       encryptedData = RSA.Encrypt(Data, DoOAEPPadding);
}
catch (CryptographicException e)
{
Console.WriteLine(e.Message);
return null;
}
}
```

FUNCTION FOR DECRYPTION:



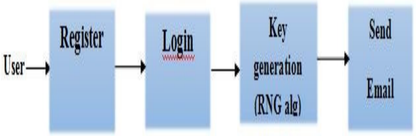
```
static public byte[] Decryption(byte[]Data, RSAParameters RSAKey, bool DoOAEPPadding)
{
try
{
byte[] decryptedData;
using (RSACryptoServiceProvider RSA = new RSACryptoServiceProvider())
  {
   RSA.ImportParameters(RSAKey);
   decryptedData = RSA.Decrypt(Data, DoOAEPPadding);
  }
return decryptedData;
}
catch (CryptographicException e)
{
Console.WriteLine(e.ToString());
return null;
}
}
```

ARCHITECTURE:

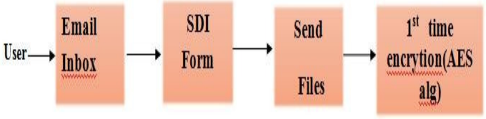


4.1 Generating secretkey:

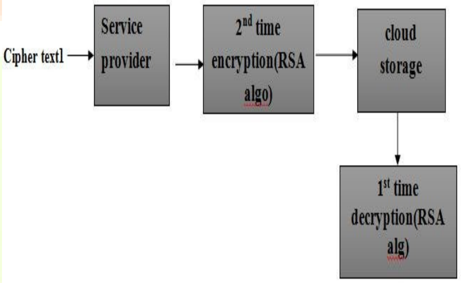
In this module, the user has to register for this Application. A security key is send to registered users. Sender first need service provider Security key which acts as an authentication key.Admin generates this secret key and it is sent to all registeredusers.



4.2 Security provider and single Encryption: In this module, user first receives theSecurity key from the admin. That securitykeyisstore in database which is used for verification. After verification of that key, then the user is connected to his/her service. The user attaches the file in mail with receiver details. Now, the first time encryption is taken place at User level by AES algorithm.

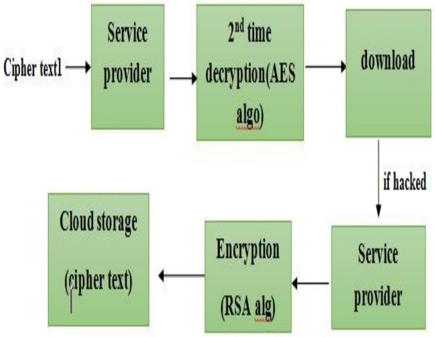


4.3 Second encryption and single decryption: Second level encryption in the service provider. Here RSA algorithm isusedforencryption. This encrypted message isstoredinCloud storage. This cloud storageconsistsofonly cipher text. After this process,themessageis sent to receiver. When the receiverreceivesthefiles, first time decryption is done by RSA algorithm.



4.4 Second decryption and downloading the data.

The second time decryption is done at user level by AES algorithm. After complete decryption, the complete file is opened by receiver. If the service provider is hacked, the cloud storage executes RSA algorithm to back up the files to secure it.



5. CONCLUSION

Cloud storage made our work challenging. The performance of the cloud may affect if whole service is done in cloud. Thus to avoid such problem this technique is used. Here, the encryption and decryption is robust. The whole data are recovered from cloud.

6. REFERENCE

[1] Two-Factor Data Security Protection Mechanism for Cloud Storage System Joseph K. Liu, Kaitai Liang, Willy Susilo, Jianghua Liu, and Yang Xiang, Senior Member,IEEE,
June 2016

[2] Privacy-Preserving Public Auditing for Secure Cloud Storage Cong Wang, Student Member, IEEE, Sherman S.-M. Chow, Qian Wang, Student Member, IEEE, KuiRen, Member, IEEE, and Wenjing Lou, Member, IEEE , Nov 2013 [3] Securing Software as a Service Model of Cloud Computing: problems and Solutions Rashmi, Dr.G.Sahoo, Dr.S.Mehfuz Birla Institute of Technology, Mesra, Ranchi, Jharkhand,India3Jamia MiliaIslamia, Delhi,India, Aug 2013 [4] Distributed, Concurrent and Independent Access to Encrypted Cloud Databases Luca Ferretti, Michele Colajanni and MircoMarchetti, feb 2014

[5] H. Guo, Z. Zhang, J. Zhang, and C. Chen, “Towards a secure certificateless proxy re-encryption scheme,” in Proc. 7th Int. Conf. Provable Security, 2013, pp. 330–346.

[6] L. Ferretti, M. Colajanni, and M. Marchetti, “Distributed, concurrent, and independent access to encrypted cloud databases,” IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 2, pp. 437–446, Feb. 2014.

[7] C.-K. Chu, S.S. M. Chow, W.-G.Tzeng,
J.Zhou, and R H. Deng, “Key-aggregate cryptosystem for scalable data sharing in cloud storage,” IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 2, pp. 468– 477, Feb. 2014