End To End Secure Data Sharing Using Cloud

N.Petchiappan
Dept of Computer Application
Sri Muthukumaran Institute Of Technology

Abstract- *Nowadays Usage of Cloud Computing is the on demand availability of computing resources. Especially data storage and data sharing. While sharing the data using cloud there comes the threat of data theft. So secure data sharing is a most important thing in todays cloud computing. We here used dual encryption method to share a data or document privately in cloud. Also we look forward through "CIA" security triad that is Confidentiality, Integrity and Availability of documents or data.*

I. INTRODUCTION

This paper discusses about security and privacy problems in cloud computing and identifies the better solution for the selected problem(data Sharing).while cloud computing is associated with numerous security and privacy problems, it can be made effective by implementing efficacious solution. In this thesis I separate cloud computing security issues from its privacy issues.

II. RESEARCH METHODOLOGY

Research methodology is a process of managing and solving research problems systematically. To Achieve the goals of research we here uses Systematic Litrature Review (SLR). It is defined as identifing, evaluating and interpreting the available relevant work for a particular phenomenon of intrest. SLR is used mainly to summarize the existing state of the art and to determine the gaps in it.

III. PROPOSED SYSTEM

There are two kinds of secret key generation such as Symmetric and Asymmetric. Symmetric deals with Data Encryption Standard(DES) and Advanced Encryption Standard (AES). While Assymmetric deals with two key generation (Public, Private) and also deals with RSA and Eliptic Curve Cryptography(ECC). Here we uses Assymmetric key generation method which is also known as Dual Encryption Method.

ALGORITHM FOR THE PROPOSED ARCHITECTURE:

3.1) Algorithm for Encryption:

Begin();
Plain text P-> t1, t2, t3,…,tn
Generate Prime number P_{xi} and $P_{xi}=2X_i$
Take sorting of P_{xi} (Q_i and R_i)
Cipher $K^{ci}_I = 2^{p+1} – K_I$;
Generaterandominteger I= d1+d2+d3+…+dn
$I_n = X_n$
if n=2
Case (I)
$y1=(x1\ Q_i * R_i + d1)$
$y2=(x1\ Q_i * R^{ci}_I + d2)$
Case (II)
$G(y1)= a\ y^2_1 +b$
$G(y2)= a\ y^2_2 +b$
End

This double encryption is expressed as follows

$$y(x)= px+q$$

3.2) ALGORITHM FOR DECRYPION:

Step 1 Apply inverse from INF
$G_I= g^{-1}\ y=^{yi-b}/i$
Step 2 Encrypted chiper text
$F1=g(y^2_1)$;
$F2=g(y^2_2)$;
Step 3 add all encrypted chiper text
Si=f1+f2
Step 4 subtract larger integer
$Z_i=S_i-I_i$
Delete zero pads
Step 5 perform the above steps for all encrypted data parts
Step 6 Convert into byte array
Step 7 Merge all Byte array
Step 8 get original plaintext()
The above algorithm is expressed as follows
$\mathbf{y^{-1}(x)= {}^{xi-q}/p}$

IV. FUNCTIONALITIES OF THE SYSTEM

- Creates Id for both the user
- Gets all information about both the user
- User1 can request for the data from User2
- User2 upload the data in a private mode in the system

- User1 search for the data using the keyword
- User1 after finding sends request for the decryption key to User2
- User2 then search for request of key and then approves it.
- Then the user1 gets mail or message with decryption key
- Using the key user1 decrypts the data and views it.

V. RESULT

In this journal we proposed double encryption-decryption mechanism also known as IDED for secure online data sharing in cloud. This mechanism is fooling the attackers even the attacker hacks the stored file he is not sure about the original data. Even though they encrypt the data due to double encryption and decryption the possibility of data secure is maximum compared to the existing technologies. Before storing of data cloud undergoes double encryption and on retrieving double decryption to get the original data.

REFERENCES

[1] B.Hauer, “data and information leakage prevention within the scope of information security” IEEE access vol 3, pp.2554-65, dec 2015.
[2] G.Sweetha, K.Suriya, R.Jothi“ Security and privacy issues in cloud computing” Emerg.trends adv. Comput., pp. 69-75 , 2015
[3] S.Haykin and M.Moher, Modern Wireless communication, Prentice Hall 2005.