Secured file storage and retrieval in cloud using cryptography with secret key

K.Kanagalakshmi, T.Sumathi

Abstract- **Cloud computing technology is very useful in present day to day life, it uses the internet and the central remote servers to provide and maintain data as well as applications. Such applications in turn can be used by the end users via the cloud communications without any installation. Moreover, the end users' data files can be accessed and manipulated from any other computer using the internet services. If the confidentiality of the information of very high value, it should be protected. If we want to stop the unauthorized disclosure or alteration of the information it should be secured. Cryptography is a technique which is used to protect the important data. It uses encryption and decryption methods. Encryption is the science of changing data so that it is unrecognizable and useless to an unauthorized person. Decryption is changing it back to its original form. This research paper is aimed to develop an algorithm with double secret keys in cloud environment. The proposed algorithm is based on AES (Advanced Encryption Standard) with additional secret key.**

Keywords: **Cloud Computing, Cryptography, Decryption, Encryption., Security,Secret Key.**

I.INTRODUCTION

In today's corporate world where access to information in lesser time is required with the goal of running the enterprise smoothly and efficiently, it is very important to give right information to right people at right time. What actually the information has been sent should be the same information been received. Suppose one person is sending an important file to the other person who is sitting at some other site office then the message passes through an insecure channel and may be possible that anyone in the middle can retrieve the message and modify it and then passes it to the destination. This will lead to many undesirable side-effects and the company may suffer a big loss in economical terms. Cryptography plays a very vital role in keeping the message safe as the data is in transit. It ensures that the message being sent at one end remains confidential and should be received only by the intended receiver at the other end [5].

Cryptography converts the original message in to non readable format and sends the message over an insecure channel. The people who are unauthorized to read the message try to break the non readable message but it is hard to do it so. The authorized person has the capability to convert the non readable message to readable one [9].

A. Cryptography

A process of converting Plain Text into Cipher Text is called as Encryption. Decryption is the process of converting Cipher Text into Plain Text. A Key is a numeric or alpha numeric text or may be a special symbol. The Key is used at the time of encryption to convert Plain Text to cipher text and at the time of decryption key is used to convert the cipher text into plain text. Based on the keys used encryption algorithms classified into two broad categories- Symmetric and Asymmetric key encryption[5].

i)Symmetric key encryption

In Symmetric key encryption, a single key is used for encryption and decryption. The key used for decryption is as same as in encryption. The algorithms used for symmetric encryption are DES, 3DES, AES [1].

ii)Asymmetric key encryption

In Asymmetric key encryption, two different keys used for encryption and decryption. One key is used for encryption and another one key is used for decryption. The algorithms used for asymmetric encryption are Rivest, Shamir, & Adleman

ISSN: 2278 – 1323

(RSA), Elliptic Curve(EC), Diffi-Hillman(DH)[2].

B. Cloud Computing

Cloud computing technology is very useful in present day to day life, it uses the internet and the central remote servers to provide and maintain data as well as applications. Such applications in turn can be used by the end users via the cloud communications without any installation. Moreover, the end users' data files can be accessed and manipulated from any other computer using the internet services. If the confidentiality of the information of very high value, it should be protected. If we want to stop the unauthorized disclosure or alteration of the information it should be secured. Cryptography technique is used to protect the important data which is stored in cloud. The data stored in the encrypted form will be secure [8].

II. PROPOSED MODEL: SECURED FILE STORAGE AND RETRIEVAL IN CLOUD USING CRYPTOGRAPHY WITH SECRET KEY

An approach to secure file storage and retrieval in cloud using cryptography has been proposed. The proposed method called "Secured file storage and retrieval in cloud using cryptography with secret key" an encryption technique is used to secure file in cloud and also secret key is used to enhance the security. In the existing system, encryption techniques alone used for file security but the proposed model uses secret key as a extra security feature while retrieving file from cloud. The proposed method consists of 5 phases. They are Register user details, User login, Secret key generation, File Encryption and Upload, File decryption and download. The system level design of the proposed model is given in the Fig 1(a),Fig 1(b).

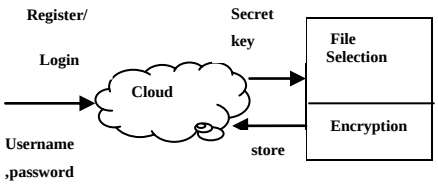

Fig. 1(a) Encrypted and Key Bound File Storage in Cloud(Upload)

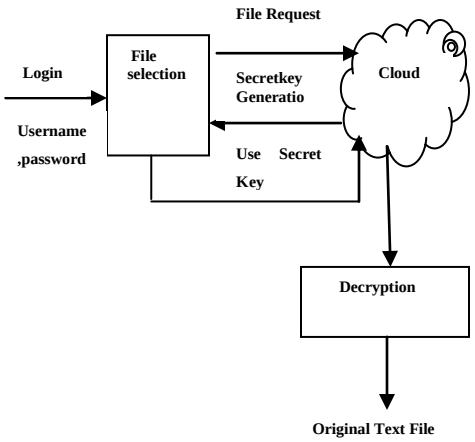

Fig. 1(b) File Retrieval from Cloud with Secret Key (Download)

A. Algorithm for proposed methodology

The algorithm of the proposed model based on Advanced Encryption Standard (AES)[3] is given below.

i. File Upload

The file can be downloaded by performing the following steps:

Step 1: Register user details in cloud

Step 2: User login using username, Password

Step 3: Secret key generation by cloud and user login using secret key

Step 4: Select file for Encryption

Step 5: Encrypt file and upload in cloud

ii. File Download

The file can be downloaded by performing the following steps:

Step 1: User login using Username, Password

Step 2: Select file for download

Step 3: Secret key generation by cloud and login using secret key to download file from cloud

Step 4: Decrypt and download file from cloud.

ISSN: 2278 – 1323

B. Register user details

The user has to register their details in cloud in order to use the storage facility of cloud. Each user has to register them by giving the details of name, password, mail id, gender, address, city, state, country, mobile number.

C. User login

If the user gets registered in the cloud then they can use the storage facility provided by the cloud. While registering the details the user has to given the username and password. User can login to the cloud using this username and password. This is the first entry level. After this entry, user has one more login using secret key.

D. Secret key generation

In the proposed model, secret key is used to enhance the security of file. Each user of cloud is provided with user name and password. While the user login to the cloud they have to enter username and password. If the username and password is correct then the user is considered to be a valid user and they can entered into the cloud.

The proposed model generates a secret key for security along with the username and password. If the user is considered to be a valid user then secret key is generated by cloud and sent to user's mail ID which is given by the user while registration. The user mail ID and password must be secret one. So secret key sent to user's mail will be secret one. The user has to open their own mail and enter the secret key which is sent to that mail. If the secret key is correct then the user can store/retrieve their files in cloud.

Each time the user login they going to receive a different secret key. So this secret key method provide security to the user's files which are stored in cloud.

Steps for secret key generation :

Step 1: User login by providing username and password

Step 2: Secret key (a random number) is generated by cloud and send to user mail ID

Step 3: User gets secret key by sign in to their mail

Step 4: User enter secret key and enter into cloud for processing their files

E. File encryption and upload

If the user successfully login to the cloud then they can encrypt and upload their files. The user has to select and encrypt their file and then upload the file into cloud storage area.

i)File Encryption

In the proposed method, the Advanced Encryption Standard (AES) algorithms used for encrypting the files.

AES Algorithm

AES algorithm is a symmetric cryptographic algorithm. So same key is used for both encryption and decryption. In the proposed system AES algorithm is used for encryption and decryption. Advanced Encryption Standard, is a symmetric block cipher that can encrypt data blocks of 128 bits using symmetric keys 128, 192, or 256. AES encrypt the data blocks of 128 bits in 10, 12 and 14 round depending on the key size. In the proposed system 128 bit key size is used. AES is an iterated symmetric block cipher. So it has the following characteristics:

· AES works by repeating the same defined steps multiple times

· AES is a secret key encryption algorithm

· AES operates on a fixed number of bytes.

AES encryption algorithms is reversible. This means that almost the same steps are performed to complete both encryption and decryption in reverse order[4][6].

Block : AES algorithm is a block cipher algorithm. This means that the number of

ISSN: 2278 – 1323

bytes that it encrypts is fixed. AES encrypt blocks of 16 bytes. If the bytes being encrypted are larger than the specified block then AES is executed concurrently. If the plain text is smaller than 16 bytes then it must be padded in order to get 16 bytes [7].

State Array : State means current condition of the block. That is the block of bytes that are currently being worked on. The block of bytes to be encrypted is stored in an array. This array is called state array[7].

XOR Operation : XOR refers to the bitwise operator Exclusive Or. XOR operates on the individual bits in a byte in the following way[7]:

0 XOR 0 = 0

1 XOR 0 = 1

1 XOR 1 = 0

0 XOR 1 = 1

Round Keys : The cipher key used for encryption is 128 bits long. It is used to generate a set of eleven 128-bit round keys that will be combined with the data during encryption. Although there are ten rounds, eleven keys are needed because one extra key is added to the initial state array before the rounds start. Round keys [6] is an array of eleven 16-byte values, each made up of four 32-bit words, as shown in Table I.

Table I: Values of Round Key Array

	32 bits	**32 bits**	**32 bits**	**32 bits**
$Rkey_0$	W_0	W_1	W_2	W_3
$Rkey_1$	W_0	W_1	W_2	W_3
$Rkey_2$	W_0	W_1	W_2	W_3
$Rkey_3$	W_0	W_1	W_2	W_3
$Rkey_4$	W_0	W_1	W_2	W_3
$Rkey_5$	W_0	W_1	W_2	W_3
$Rkey_6$	W_0	W_1	W_2	W_3
$Rkey_7$	W_0	W_1	W_2	W_3
$Rkey_8$	W_0	W_1	W_2	W_3
$Rkey_9$	W_0	W_1	W_2	W_3
$Rkey_{10}$	W_0	W_1	W_2	W_3

Steps for calculating Round Keys :

Step 1: The first round key $Rkey_0$ is initialized to the value of the cipher key. Each of the remaining ten keys is derived from this as follows.

Step 2: For each of the round keys $Rkey_1$ to $Rkey_{10}$, words W_1, W_2, W_3 are computed as the sum of the corresponding word in the previous round key and the preceding word in the current round key.

For example, using XOR for addition:

$Rkey_5$: $W_1 = Rkey_4{:}W_1$ XOR $Rkey_5{:}W_0$,

$Rkey_8$: $W_3 = Rkey_7{:}W_3$ XOR $Rkey_8{:}W_2$ and so on.

For each round key $Rkey_1$ to $Rkey_{10}$, the value of W_0 is the sum of three 32-bit values:

- The value of W_0 from the previous round key

ISSN: 2278 – 1323

- The value of W_3 from the previous round key, rotated right by 8 bits
- A special value from a table called Rcon

Thus, $Rkey_i:W_0 = Rkey_{(i-1)}:W_0$ XOR $(Rkey_{(i-1)}:W_3 >>> 8)$ XOR Rcon[i]

where W >>> 8 means rotate right 8. Rcon[i] is an entry [6] in Table II.

Table II Values in Rcon Table of Algorithm

Iteration(i)	Rcon(i)
1	2
2	4
3	8
4	16
5	32
6	64
7	128
8	27
9	54
10	108

Encryption

The Encryption process of AES Algorithm contains the following steps.

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

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

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 out as the encrypted data (ciphertext).

Computing the Rounds

The following operations used in computing each round.

- SubBytes
- ShiftRows
- MixColumns
- XorRoundKey

Each one of these operations is applied to the current state array and produces a new version of the state array. In the first nine rounds of the process, the four operations are performed in the order listed. In the last (tenth) round, the MixColumns operation is not performed and only the SubBytes, ShiftRows, and XorRoundKey operations are done.

SubBytes : This operation is a simple substitution that converts every byte into a different value. AES defines a table of 256 values for the substitution. The state array contains 16 bytes and each byte is replaced by the value from the substitution table.

ShiftRows : ShiftRows operates on each row of the state array. Each row is rotated to the right by a certain number of bytes as follows:

1^{st} Row: rotated by 0 bytes (i.e., is not changed)

2^{nd} Row: rotated by 1 byte

3^{rd} Row: rotated by 2 bytes

4^{th} Row: rotated by 3 bytes

MixColumns : Each column of the state array is processed separately to produce a new column. The new column replaces the old one. The processing involves a matrix multiplication. The MixColumns operation takes each column of the state array C_0 to C_3

ISSN: 2278 – 1323

and replaces it with a new column computed by the matrix multiplication[6] shown below.

$$\begin{bmatrix} C'_0 \\ C'_1 \\ C'_2 \\ C'_3 \end{bmatrix} = \begin{bmatrix} 02 & 01 & 01 & 03 \\ 03 & 02 & 01 & 01 \\ 01 & 03 & 02 & 01 \\ 01 & 01 & 03 & 02 \end{bmatrix} \bullet \begin{bmatrix} C_0 \\ C_1 \\ C_2 \\ C_3 \end{bmatrix}$$

The new column is computed as follows:

$C'_0 = 02 * C_0 + 01 * C_1 + 01 * C_2 + 03 * C_3$

$C'_1 = 03 * C_0 + 02 * C_1 + 01 * C_2 + 01 * C_3$

$C'_2 = 01 * C_0 + 03 * C_1 + 02 * C_2 + 01 * C_3$

$C'_3 = 01 * C_0 + 01 * C_1 + 03 * C_2 + 02 * C_3$

XorRoundKey : This operation takes the existing state array, XORs the value of the appropriate round key, and replaces the state array with the result. It is done once before the rounds start and then once per round, using each of the round keys in turn**.**

Decryption

Decryption involves reversing all the steps taken in encryption using inverse functions:

- InvSubBytes
- InvShiftRows
- InvMixColumns

XorRoundKey doesn't need an inverse function because XORing twice takes back to the original value. InvSubBytes works the same way as SubBytes but uses a different table[4] that returns the original value. InvShiftRows involves rotating left instead of right and InvMixColumns uses a different constant matrix to multiply the columns.

Steps for Decryption :

Step 1: Perform initial decryption round in the following order:

XorRoundKey

InvShiftRows

InvSubBytes

Step 2: Perform nine full decryption rounds in the following order:

XorRoundKey

InvMixColumns

InvShiftRows

InvSubBytes

Step 3: Perform final XorRoundKey The same round keys are used in the same order.

ii)File Upload

The cloud is providing security for the user using encryption techniques. User files are stored in the cloud in the encrypted format. So nobody can see the data in the file except owner of the file who is actually know how to decrypt the file. For encryption AES(Advanced Encryption Standard) algorithm is used.

F. File Decryption and Download

Once the user get registered in the cloud they can login anytime and stored their files. The files are stored in the encrypted format. If the user want to see the files means they have to perform the following steps:

Step 1: Login to the first entry of the cloud using username and password

Step 2: Login to the second of the cloud using secret key

Step 3: Select the file to download

ISSN: 2278 – 1323

Step 4: Enter the secret key which is sent to user's mail id

Step 5: Download the file.

III EXPERIMENTAL RESULTS AND FINDINGS

The proposed encryption technique for secured file storage/retrieval in cloud have been implemented in C# .NET, ASP .NET and experimental results are observed.

The User of the cloud must register their details before entering into cloud. There after only user can use storage facility provided by the cloud. The user has to register their name, password, email id etc., After registration, File Uploading and Downloading process have been carried out.

A. File Upload

The user can login to the cloud using the username and password given by them while registering details. If the username and password is valid and then the user navigate to page shown in the Fig.2. This page require secret key which is sent to user's personal mail id. The mail id is given by the user while registering.

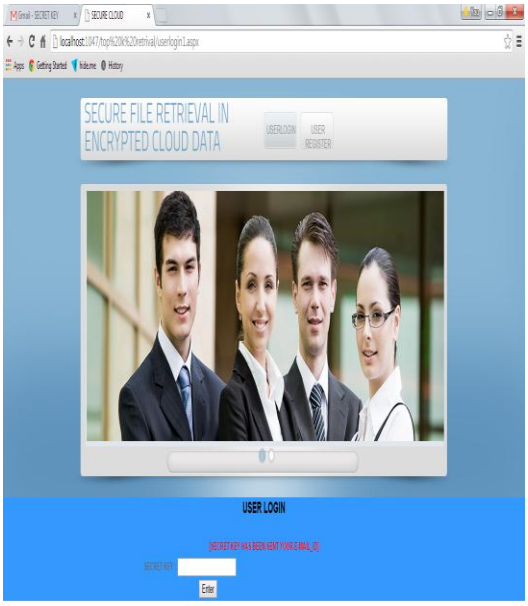

Fig.2 View of userlogin1 page before entering secret key

Secret key sent to user's mail id is shown below in Fig.3. The key is generated by the cloud when the user tries to store the file. The user can obtain the secret key from their mail box.

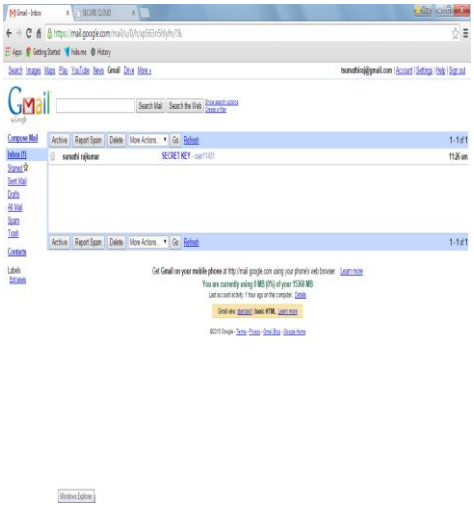

Fig.3 View of user email(Inbox) which contains secret key

The user has to enter secret key which is obtained from his/her email. If the secret key is valid then the user navigate to their home page. In home page, user can upload files by choose 'FILE UPLOAD' or download their files using 'FILE DOWNLOAD'. The user can upload their files by choosing them as in Fig.4.

Fig.4 View of fileupload page before choose file to upload

ISSN: 2278 – 1323

The user can browse and select file for upload.Fig.5 is displaying file content which is chosen for upload. The user can encrypt their file using 'ENCRYPT' option. The file can be encrypted and shown in the text area as in Fig.6.

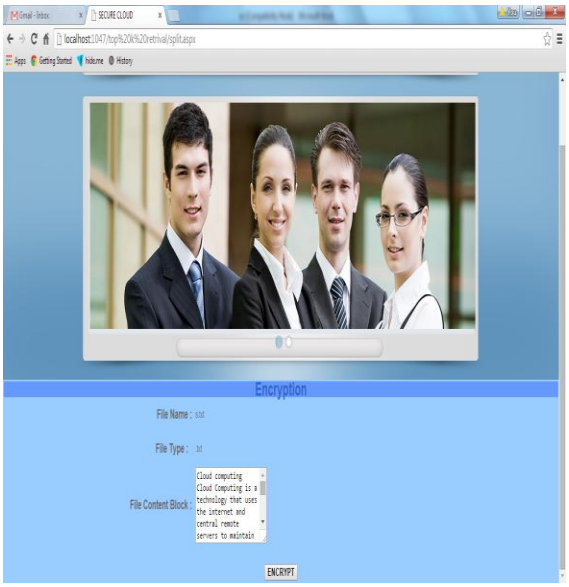

Fig.5 View of split page shows file content before encryption

Fig.6 View of filup2 page which shows encrypted content and used to upload file

B. File Download

The following figures 7,8,9 highlights the downloading activities required to be done to securely download their files. User has to select 'FILE DOWNLOAD' to download their files in the user home page. The needed file can be then chosen 'VIEW'. The content of the file is shown in encrypted form. User has to enter secret key which is sent to their email to download file.

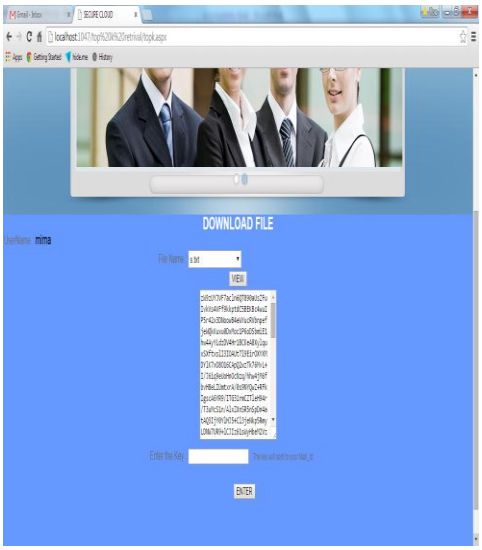

Fig.7 View of topk page after user select s.txt file to download and click 'VIEW' button

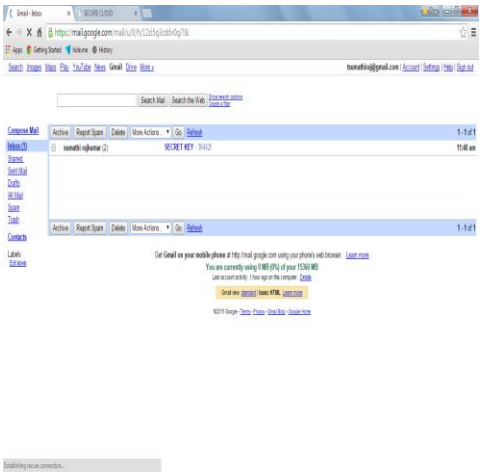

Fig.8 View of user's email(Inbox) which contains the secret key to download file

If the secret key is valid then the user can download their file by clicking 'DOWNLOAD' button as given in Fig.9.

ISSN: 2278 – 1323

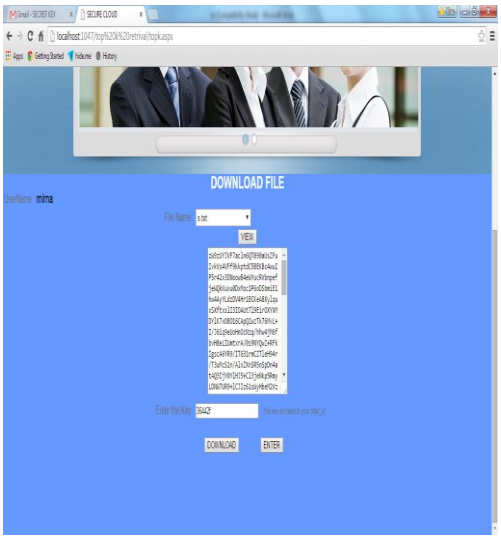

Fig.9 View of topk page which display 'DOWNLOAD' button if secret is correct

C. Security Analysis

The security factor has been enforced and improvised by introducing addition key. This key is generated by the cloud using random number generation technique. The experimental results showed that how the cloud users can acquire security for their data and how securely access those data.

IV. CONCLUSION

Cloud computing is one of the most important way that allow us to share distributed resources now a days. Although cloud computing provides a number of advantages that include economies of scale, dynamic provisioning, increased flexibility and low capital expenditures, it also introduces a range of new security risks. Thus, to take full advantage of the power of cloud computing, end users need comprehensive security solutions to attain assurance of the cloud's treatment of security issues. The cryptographic techniques will be a best solution for that security issue. The proposed system of "secured file storage and retrieval in cloud using cryptography techniques with secret key" will be more secure because of encryption techniques and random secret key generation.

REFERENCES

[1] Ayushi," A Symmetric Key Cryptographic Algorithm", International Journal of Computer Applications, Vol 1 No. 15, PP.0975 – 8887, 2010.

[2] Hamdan.O.Alanazi, B.B.Zaidan, A.A.Zaidan, Hamid A.Jalab, M.Shabbir and Y. Al-Nabhani, "New Comparative Study Between DES, 3DES and AES within Nine Factors", Journal of Computing, Vol 2, Issue 3, PP.152-156, March 2010.

[3] Ohyoung Song, and Jiho Kim, "Compact Design of the Advanced Encryption Standard Algorithm for IEEE 802.15.4 Devices", Journal of Electrical Engineering & Technology Vol. 6, No. 3, pp. 418-422, 2011.

[4] Punita Mellu, Sitender Mali, "AES: Asymmetric key cryptographic System", International Journal of Information Technology and Knowledge Management, Vol, No. 4, PP. 113-117, 2011.

[5] Sumedha Kaushik, Ankur Singhal, "Network Security Using Cryptographic Techniques", International Journal of Advanced Research in Computer Science and Software Engineering, Vol 2, Issue 12, PP. 105-106, December 2012.

[6] BaltimoreTechnologies,"Technical Overview of RJINDAEL –The AES", http://dev.baltimore.com/aes/tech_overview.html

[7] "RijndaelEncryption", http://tropsoft.com/strongenc/rjindael

[8] Cloud Computing https://wiki.cloudsecurityalliance.org/guidance/index.php/Cloud_Computing_Architectural_Framework

[9] Cryptography www.**cryptography**world.com/**concept**.htm

Dr.K.Kanagalakshmi,

Associate Professor, PG Department of Computer Application,Vidyasagar College of Arts and Science, Udumalpet.

Mrs.T.Sumathi,

Research Scholar, Department of Computer Science,Vidyasagar College of Arts and Science, Udumalpet.

ISSN: 2278 – 1323