Enhancing Data Security in the Cloud using Security (RSA) Algorithm

*Vishwanath S. Mahalle,
9421494320, vsmahalle@gmail.com
Faculty of C.S.E. Department, Shree
Sant Gajanan Maharaj College of
Engineering, Shegaon.

Ritesh Satija,
8275355563, ritesh.21satija@gmail.com,
Final Year Student of C.S.E.,
Shree Sant Gajanan Maharaj College of
Engineering, Shegaon.

ABSTRACT

Security being the most important factor in cloud computing has to be dealt with great precautions. Thus to provide security to the user data in cloud we make use of RSA algorithm. We have focused on following key tasks:

1. Secure Upload of data on cloud such that even the vendor is unaware of the contents.
2. Secure Download of data in such a way that the integrity of data is maintained.
3. Proper usage and sharing of the public and private keys involved for encryption and decryption.

The use of a single key for both encryption and decryption is very prone to malicious attacks. But in RSA, this problem is solved by the use of two separate keys one each for encryption as well as decryption. Out of the two keys one is the public key, which is made available to all and the second one is the private key which lies only with the user. In this way, both the secure upload as well as secure download of the data is facilitated using the two respective keys. Also, the key generation technique used in this project is unique in its own way. This has helped in avoiding any chances of repeated or redundant key.

INTRODUCTION

Computer in its evolution form has been changed multiple times, as learned from its past events. From the beginning, mainframes were predicted to be the future of computing. Indeed mainframes and large scale machines were built and used, and in some circumstances they are used similarly today. The trend, however, turned from bigger and more expensive, to smaller and more affordable commodity PCs and servers which are tied together to construct the so called Cloud Computing System, denoted as Cloud in short, due to their same capability in providing services, say storage, computation, and management and so on.

The internet or online connectivity started out as a simple information exchange. Almost anything that users want to learn is possible because of the internet. They just need to go online, make a few searches and in a minute or two; they have the information they need. Personal communication became a lot easier as email was developed as one of the greatest innovations of the century. Instead of sending a snail mail which could take weeks, a single email could be read in a matter of seconds. Even with a simple connection, exchange of information could be done - chat and updates on new data can also be done through the internet. Although the same things could be done without internet, the experience that comes from internet has become so much more. Through improvement of communications infrastructure, the internet was able to move away from the regular phone line and now has a dedicated connection. Dial-up connection is almost a thing of the past as most of the household have adapted the dedicated lines with increasing internet connection. Wireless connectivity with almost the same speed is also possible. You do not need to drag a cable around; you just have a decent internet connection.

Cloud computing is everywhere. Pick up any technical magazine or visit almost any IT website or blog and you will be sure to see a talk about Cloud Computing. The only problem is that not everyone agrees on what it is. Ask ten different IT professionals what Cloud Computing is, and you'll get ten different answers.

Problem Statement

Encryption algorithms became much more complex to combat brute forcing. However, new issues arose. In symmetric key encryption, the recipient would also have to know the sender's key in order to decode the message. If anyone intercepted this key, all of the messages would be compromised until we changed it. Even then, the interceptor could simply steal the key again. Therefore, even the most complex algorithms following this method were easily broken. But RSA Algorithm is a form of public key encryption. Public key encryption is a process where each user is given two keys, one of which is a public and seen by anyone who wishes to see it and one which is kept strictly private. The thought of making one of the keys public seems bizarre at first, but we will soon see why this is so effective and secure. When using symmetric algorithms, both parties share the same key for encryption and decryption. To provide privacy, this key needs to be kept secret. Once somebody else gets to know the key, it is not safe anymore. Symmetric algorithms have the advantage of not consuming too much computing power. Asymmetric algorithms seem to be ideally suited for real-world use: As the secret key does not have to be shared, the risk of getting known is much smaller. Every user only needs to keep one secret key in secrecy and a collection of public keys that only need to be protected against being changed.

In RSA, each message is encrypted using the recipient's public key. We can get the recipient's public key easily - it's public. However, only the recipient has the corresponding private key to decode it. So suppose someone intercepted the message. They would only have access to the public keys, but almost no way to actually decrypt the message.

a. Existing System

The role of Cloud vendor is to store the data and information of the customer but there are number of security concerns due to which clients hesitate in storing their data in cloud. In most cases, the provider must ensure that their infrastructure is secure and that their clients' data and applications are protected while the customer must ensure that the provider has taken the proper security measures to protect their information. The cloud vendors generally store the client's data and information in cloud without following any security measures.

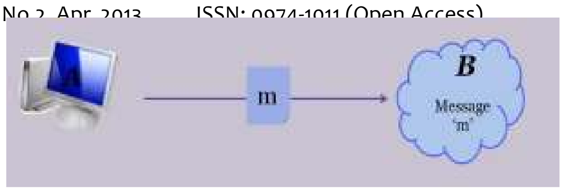


Fig: Data Uploaded in Cloud

As a result, the client's data in cloud becomes vulnerable for access by an intruder easily. Now, the client's data which is possible to be accessed by any undesired third party may lead to great loss of the company if it happens in case.

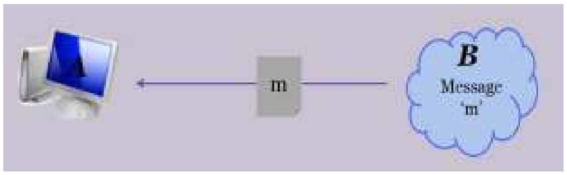


Fig: Data Downloaded from Cloud

Almost every cloud provider does not provide enough security measures to ensure the data safety and that's why clients waver keeping their data at some place which is very easy to be accessed by someone else.

b. Proposed System

The proposed system is implemented in Eyeos that is one of the cloud providers. In order to apply security features, RSA algorithm is used which is using 1024 bit RSA key. As soon as user logins in Eyeos, it gets directed to its welcome page which generates keys using random mouse movement within the particular java applet area. Now, as the key generation gets completed, the user name and public keys are stored in the database and the private key is kept secretly by the user. Now, after completing this process, user can go for storing its private data on the cloud. As soon as user tries to upload the data on cloud, the data is first stored in a temporary directory and finally encrypted by using the public key of cloud and stored in the cloud in its encrypted form.

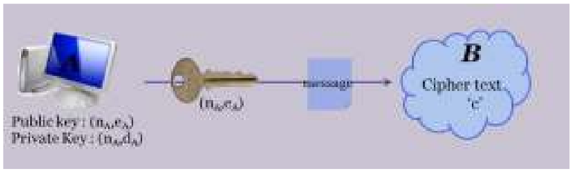


Fig: Data Uploaded in Cloud

Now, when the user wants to access the data stored in cloud or wants to download the data, it goes through the download procedure whereby user has to specify the filename to be downloaded and has to provide the private key which is kept secret by the user and is known only to him. As soon as the user asks for downloading the file, the particular encrypted file stored in the cloud is decrypted and downloaded at the user side. At the same time, the decrypted file stored in the cloud is deleted so that no further attempt to access the file could be made by any intruder. Thus, the data is stored in the cloud and finally downloaded by the user in a very secure way.

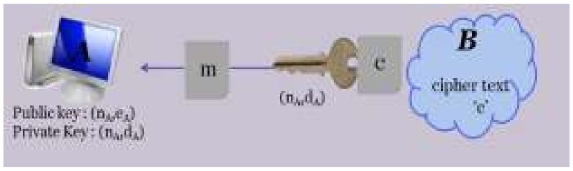


Fig: Data Downloaded from Cloud

MATERIALS AND METHODS

I propose following three modules:

I. Registration Module
II. Upload Module
III. Download Module

I. Registration Module:

It consists of two parts:

i. Account Creation:

User creates his account on the cloud by providing his details and a unique username along with a password for his account.

ii. Key Generation:

A key generation wizard is invoked when user logins for the first time. It prompts user to move the mouse pointer in the given specified area. The wizard gives two public and one private key with the help of this random movement of the mouse. User keeps his private key with himself and allows cloud to store both the public keys in the database.

II. Upload Module:

It consists of three parts:

i. Authentication:

User authenticates himself to the Cloud with his unique username and the password.

ii. Upload:

This module allows user to upload his files or any data in a secure way. User searches the data he wants to upload in his file system and then uploads the encrypted form of that data in his document directory of cloud through this gateway.

iii. Encryption:

The data after uploading is first stored in the temporary file of the server that is in the Cloud. This module then helps to encrypt the data by using the public key of the user and stores the encrypted form of data in the documents of the user. The temporary files are then unlinked.

III. Download Module:

It consists of two parts:

i. Decryption:

When user wants to download his secure data, he is prompted to enter his user name along with the secret private key. By using the private key of the user the cloud decrypts the data he wants to download.

ii. Download:

Cloud sends the decrypted data to the user thereby giving the user his original data. Then the decrypted data is unlinked from the Cloud forever. Thus the data downloaded is only with the user and the cloud cannot access it in any way.

ALGORITHMS

The various algorithms used for the modules work are as follows:

I. Key Generation Module:

Following are the two procedures under this module:

primeNoSelection()

[This procedure is used to generate two distinct prime numbers P and Q of specified length (i.e. bigger than the size of integer) using movement of mouse]

```
i.    Select an area for mouse movement
      such that length(Xcoordinate) =
      length(Ycoordinate) at any point
      between the area.
ii.   Set XSTRING = NULL
iii.  Set YSTRING = NULL
iv.   Repeat (v) to (xi) until
      length(XSTRING) != specified length
```

```
v.     IF(mouse pointer is in area)  Then
vi.     XSTRING = concat(XSTRING,
        getXcoordinate);
vii.    YSTRING = concat(YSTRING,
        getYcoordinate);
viii.  Wait(50)
ix.    ELSE
x.      ENDIF
xi.     P =stringToBigInteger(XSTRING)
xii.   Q =stringToBigInteger(YSTRING)
xiii.  Repeat (xiv) until prime(P) != TRUE
xiv.    P = P + Biginteger("1")
xv.    Repeat (xvi) until prime(Q) != TRUE
xvi.    Q = Q + Biginteger("1")
xvii.  DONE.
```

keyGenerator(P,Q)

[This procedure is used to generate RSA public key, private key pair by using two big prime integers P and Q, E is Public key and D is Private Key]

```
i.     N = P * Q
ii.    PHI = (P –  1) * (Q – 1)
iii.   Take E, a BigInteger value of length
       length(N) – 1
iv.    Repeat (v) until gcd(E,PHI) != 1
v.     E = E + 1
vi.    D = modInverse(E, PHI)
vii.   Publish E as Public key and D as
       Private key
viii.  Done
```

II. Upload Module

Following are the three procedures under this module:

Uploadfile()

[This procedure uploads desired file in the cloud by encrypting the contents of file and storing it in cloud.]

```
i.     START
ii.    Retrieve  username and filename from user
iii.   Check for validity of file
iv.     IF file already exists on cloud THEN
v.      Display ERROR_MESSAGE
vi.    ELSE  upload file to temporary directory
vii.   Open file in read mode, FD :=
       open(FILENAME)
viii.  Open file in  append mode, FD1 :=
       open(concat(FILENAME,X))
ix.    CALL Encryption(FD,FD1,USERNAME)
x.     close FD
xi.    close FD1
xii.   Move FD1 file from temporary directory
       to Documents.
xiii.  Unlink FD file from temporary directory.
xiv.   END
```

Encryption(FILENAME,USERNAME,PUBLIC KEY)

[This procedure encrypts the input file by taking username,filename from user and public key fstored in the database generated by the keygenerator]

```
i.     Read file in FD
ii.    Retrieve PUBLIC_KEY_E and
       PUBLIC_KEY_N from database with the
       help of USERNAME
iii.   WHILE FD!=EOF
iv.    FOR (i = 0 to i = 41) and (fd != EOF)
v.     CALL Stringtoascii_conversion()
vi.     Set ASCIISTRING:=
       concat(ASCIISTRING,OFFSET)
vii.   END FOR
viii.  NUM=stringToInteger(ASCIISTRING)
ix.    Set ENCRYPT := [$NUM^{PUBLIC\_KEY\_E}$ ]
       mod[PUBLIC_KEY_N]
x.     Set TEMPVAR :=
       integerToString[ENCRYPT]
xi.    Write TEMPVAR to FD1
xii.  Write a Delimiter '|' to FD1
xiii.  DONE.
```

Stringtoascii_conversion()

[This procedure is used to convert contents of file to ascciistring which is further used in encrypting the file contents]

```
i.     START
ii.    Set   ASCII_VAL  :=  ascii  value  of  the
       character read from file
iii.   set ASCII_VAL:= ASCII_VAL+ offset
iv.    Return ASCII_VAL
v.     END
```

III. Download Module:

Following are the three procedures under this module:

download()

[This procedure sends the decrypted file to user]

```
i.     Retrieve USERNAME, FILENAME,
       PRIVATE_KEY from user
ii.    Check for validity of data entered by user
iii.   IF (valid data) THEN
```

```
iv.    Call decryption(FILENAME,
       USERNAME, PRIVATE_KEY)
v.     ENDIF
vi.    Setting proper header for downloading of
       decrypted file
vii.   Unlink the decrypted file
viii.  DONE.
```

decryption(FILENAME, USERNAME, PRIVATE_KEY)

[This procedure is used to decrypt the given file with the help of RSA PRIVATE_KEY, PUBLIC_KEY_N and RSA decryption algorithm]

```
i.     Retrieve PUBLIC_KEY_N from database
       using USERNAME
ii.    Open file for reading, FD1 =
       open(FILENAME)
iii.   Open another file for writing, FD2 =
       open(substr(FILENAME,-1))
iv.    Repeat (v) to (ix) until FD1 != EOF
v.     Repeat (vi) and (vii) until CH = '|'
vi.     NUM = concat(NUM, CH)
vii.    Read a character from FD1 into CH
viii.   ASCIISTRING = $(NUM^{PRIVATE\_KEY})$ mod
       (PUBLIC_KEY_N)
ix.     Call STRS =
       asciiToString(ASCIISTRING)
x.      Write STRS to FD2.
xi.    Close FD1 and FD2
xii.   DONE.
```

asciiToString(ASCIISTRING)

[This procedure is used to convert ASCII value to String which is further used in decrypting the file contents]

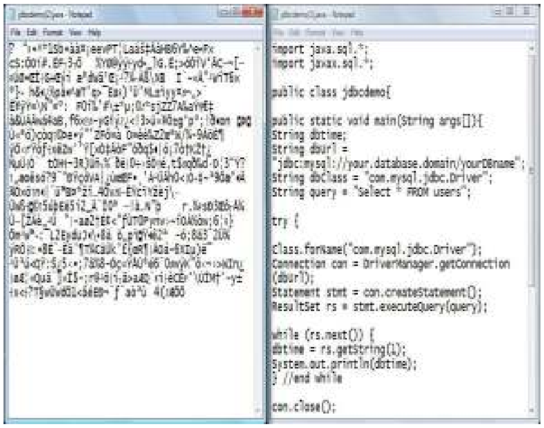
```
i.     Declare STRS, OFFSET
ii.    FOR(I = 0;I < length(ASCIISTRING); I =
       I + 3)
iii.   STR1 = "";
iv.    STR2 = "";
v.     STR1 = substr(ASCIISTRING, I , 3)
vi.    STR1 = STR1 – OFFSET
vii.   STR2 = char(STR1)
viii.  STRS = concat(STRS, STR2)
ix.    END FOR
x.     Return STRS.
```

RESULT AND DISCUSSION

i. User generates the keys with the help of the random movement of the mouse in the given specified area so it is practically impossible to generate the two same keys.

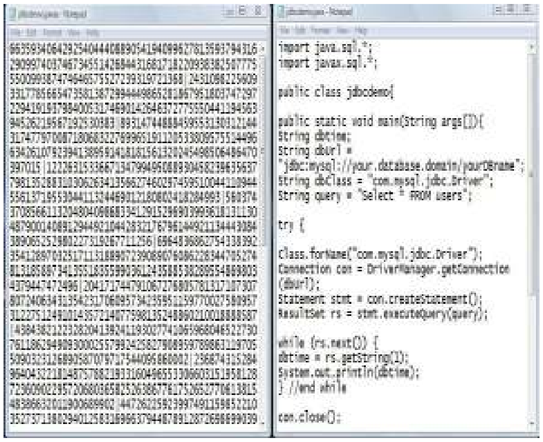
ii. 1024 bit of RSA keys are used, so one cannot guess the private key with the help of the public keys generated.

iii. If a user logins and forgets to log out or leaves the system idle. In that case if a trespasser tries to download the data from the system then that person will be asked to enter the private key. In any case if a trial to guess that private key and then try to download, he will get the data as seen on the left side of the diagram shown below. He will not get the original data.



```
import java.sql.*;
import javax.sql.*;

public class jdbcdemo{

public static void main(String args[]){
String dbtime;
String dbUrl =
"jdbc:mysql://your.database.domain/yourDBname";
String dbClass = "com.mysql.jdbc.Driver";
String query = "Select * FROM users";

try {

Class.forName("com.mysql.jdbc.Driver");
Connection con = DriverManager.getConnection
(dbUrl);
Statement stmt = con.createStatement();
ResultSet rs = stmt.executeQuery(query);

while (rs.next()) {
dbtime = rs.getString(1);
System.out.println(dbtime);
} //end while

con.close();
```

iv. To download the data in a secure way the user is always required to enter the private key. Since the private key is secret it is not even known to the Cloud's Administrator. Thus, the main advantage of proposed system is that even the Cloud's Administrator cannot access the data of the user. In case he tries to see the data he will see it in the encrypted form as seen on the left side of the figure shown below.



```
import java.sql.*;
import javax.sql.*;

public class jdbcdemo{

public static void main(String args[]){
String dbtime;
String dbUrl =
"jdbc:mysql://your.database.domain/yourDBname";
String dbClass = "com.mysql.jdbc.Driver";
String query = "Select * FROM users";

try {

Class.forName("com.mysql.jdbc.Driver");
Connection con = DriverManager.getConnection
(dbUrl);
Statement stmt = con.createStatement();
ResultSet rs = stmt.executeQuery(query);

while (rs.next()) {
dbtime = rs.getString(1);
System.out.println(dbtime);
} //end while

con.close();
```

CONCLUSION

This study proposed an RSA encryption algorithm using 1024 bit RSA key for providing data security to the user in the

Cloud. The biggest advantage it provides us is that the keys are generated randomly and so no intruder can even guess them thereby giving us increased security along with convenience. Private Key is only known to the user and therefore user's private data is not accessible to anyone not even the Cloud's Administrator. The main purpose behind using RSA encryption algorithm is that it provides two keys i.e. public key for encryption and private key for decryption. The data after uploading is stored in an encrypted form and can be only decrypted by the private key of the user. The main advantage of this is that data is very secure on the cloud. Thus its security is based on the fact that there is no efficient way to factor very large numbers. The main focus of work was to maintain the confidentiality of the data of the user which is supposed to be stored at some remote location in Cloud by a cloud vendor. Among the many IT giants, being driven by trends in cloud computing is not doubtful. The various security issues that hinder the progress and wide spread use of cloud computing can be addressed using the algorithms and techniques available. For enterprises, cloud computing is worthy of consideration and try to build business systems as a way for businesses in this way can undoubtedly bring about lower costs, higher profits and more choice; for large scale industry. The clouds will grow in size as soon as available bandwidth and the corresponding service model mature enough, cloud computing will bring a revolutionary change in the Internet. Cloud computing announced a low-cost supercomputing services to provide the possibility, while there are a large number of manufacturers behind, there is no doubt that cloud computing has a bright future.

REFERENCES

[1] Uma Somani, Kanika Lakhani, Manish Mundra "Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing" 2010 1st International Conference on Parallel, Distributed and Grid Computing (PDGC) – 28-30 Oct, 2010 IEEE

[2] (U.S.) Nicholas. Carr, fresh Yan Yu, "IT is no longer important: the Internet great change of the high ground - cloud computing," The Big Switch:Rewining the World, from Edison to Google, , CITIC Publishing House, October 2008

[3] Ya-Qin Zhang, the future of computing in the "cloud - Client", The Economic Observer reported, http://www.sina.com.cn, 2008 Nian 07 Yue 12 Ri

[4] Wang Haopeng (Air Force Aviation University of Computer Teaching, Jilin, Changchun 130022, China); Liu strong (Air Force Air University, Research Department, Jilin, Changchun 130022, China), virtualization technology in the application of cloud computing, 2008 Year