



INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

IMPLEMENTING RSA ENCRYPTION ALGORITHM TO ENHANCE THE DATA SECURITY OF CLOUD IN CLOUD COMPUTING

VISHWANATH S. MAHALLE,

Shree Sant Gajanan Maharaj College of Engineering, Shegaon, Faculty of Computer Science Department

Accepted Date:

27/02/2013

Publish Date:

01/04/2013

Keywords

Cloud
RSA Algorithm
Key Generation
Private Key
Public key
Authentication
Encryption

Corresponding Author

Mr. Vishwanath S.
Mahalle

Abstract

This paper presents RSA encryption algorithm to safeguard data security in Cloud. Security being the most important factor in cloud computing has to be dealt with great precautions. The work in this paper focused on the 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 paper is unique in its own way.

INTRODUCTION

Computer in its evolution form has been changed multiple times, as learned from its past events. Turning to Cloud Computing, 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 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.

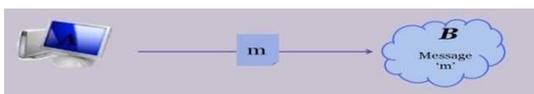


Fig: Data Uploaded in Cloud

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.

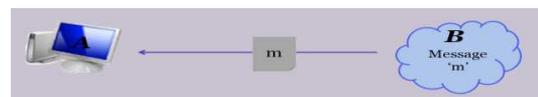


Fig: Data Downloaded from Cloud

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.

Proposed System

In order to apply security features, RSA algorithm is used which is using 1024 bit RSA key. As soon as user logs in Cloud, 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.

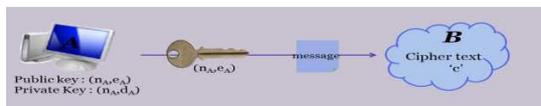


Fig: Data Uploaded in Cloud

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.

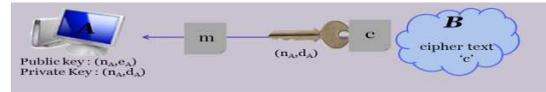


Fig: Data Downloaded from Cloud

MATERIALS AND METHODS

Paper proposes 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 logs in 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.

I (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 $\text{length}(X\text{coordinate}) = \text{length}(Y\text{coordinate})$ at any point between the area. (ii) Set XSTRING = NULL; Set YSTRING = NULL (iii) Repeat (iv) to (x) until $\text{length}(X\text{STRING}) \neq \text{specified length}$ (iv) IF(mouse pointer is in area) Then (v) XSTRING = concat(XSTRING, getXcoordinate); (vi) YSTRING = concat(YSTRING,getYcoordinate);(vii) Wait(50)Else

ENDIF P=stringToBigInteger (XSTRING) (viii)
Q =stringToBigInteger (YSTRING) (ix) Repeat
(x) until prime (P) != TRUE (x) P = P +
BigInteger ("1") (xi) Repeat (xvi) until
prime(Q) != TRUE (xii) Q = Q +
BigInteger("1") 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 $\text{length}(N) - 1$ (iv)
Repeat (v) until $\text{gcd}(E, \Phi) != 1$ (v) $E = E + 1$
(vi) $D = \text{modInverse}(E, \Phi)$ (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; Retrieve username and filename
from user (ii) Check for validity of file (iii) IF
file already exists on cloud THEN (iv) Display
ERROR_MESSAGE (v) ELSE upload file to
temporary directory (vi) Open file in read

mode, FD := open(FILENAME) (vii) Open file
in append mode, FD1 := open(concat
(FILENAME,X)) (viii) CALL Encryption
(FD,FD1,USERNAME) (ix) close FD (x) close
FD1 (xi) Move FD1 file from temporary
directory to Documents. Unlink FD file from
temporary directory. 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. (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)
END FOR (vii) NUM=stringTo
Integer(ASCIISTRING) (viii) Set ENCRY
PT:=[NUM^{PUBLIC_KEY_E}mod[PUBLIC_KEY_N]
(ix) Set TEMPVAR := integer To
String[ENCRYPT] (x) Write TEMPVAR to
FD1(xi) Write a Delimiter '|' to FD1
- ii. DONE.

III. Download Module:

Following are the three procedures under this module:

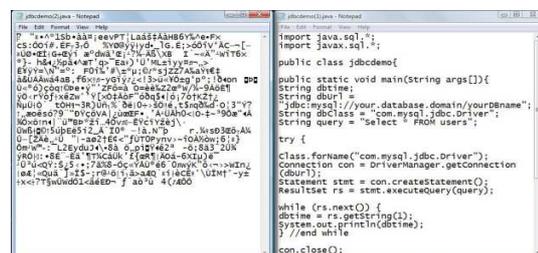
download() [This procedure sends the decrypted file to user] (i) Retrieve USERNAME, FILENAME, PRIVATE_KEY from user (ii) Check for validity of data entered by user (iii) IF (valid data) THEN (iv) Call decryption(FILENAME, USERNAME, PRIVATE_KEY) (v) ENDF (vi) Setting proper header for downloading of decrypted 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 = '|' (viii) NUM = concat(NUM, CH) (ix) Read a character from FD1 into CH (x) ASCIISTRING = (NUM^{PRIVATE_KEY})mod(PUBLIC_KEY_N) (xi) Call STRS = asciiToString (ASCII STRING) (xii)

Write STRS to FD2. (xiii)Close FD1 and FD2 (xiv) DONE.

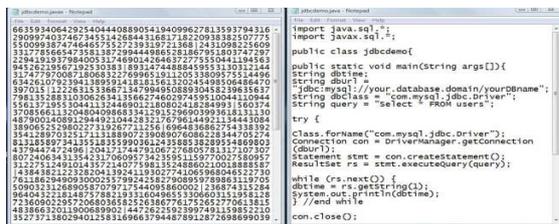
RESULT AND DISCUSSION

- 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 logs in 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.



(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.



CONCLUSION

This paper 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.