

# International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2015

## Improving Data Security in Cloud Computing Using RSA Algorithm and MD5 Algorithm

Shreya Srivastav<sup>1</sup>, Neeraj Verma<sup>2</sup>

M. Tech Scholar, Department of CSE, Om Institute of Technology and Management, Juglan, Hisar, Haryana, India<sup>1</sup>

Assistant Professor and Head of Department, Department of CSE, Om Institute of Technology and Management,  
Juglan, Hisar, Haryana, India<sup>2</sup>

**ABSTRACT:** In today's era cloud computing becomes the most emerging technology due to the ease of access to its services which it provides on demand over internet on pay per use pattern. The services provided by the cloud computing includes data storage, network services, software applications, platforms etc. without physically acquiring them which saves the managing and maintenance cost. Although this is a most promising technology for any kind of services which it generally provides but still there is one major drawback in it i.e. the security of data in cloud's environment. This is the main reason which becomes the real obstacle for people to use cloud services, as they are doubtful about the security of their data so people needs the data security in cloud paradigm. So to provide data security in cloud environment and make people more confident while using the services of cloud computing we proposed our work in which we improve the security of data in cloud computing by using RSA (Rivest, Shamir, Adleman) Algorithm and MD5 hash generation algorithm. We implement these algorithms for the security of data by using MATLAB tool.

**KEYWORDS:** Cloud computing, RSA, MD5, Hash generation, Encryption, Decryption, Data Security

### I. INTRODUCTION

#### What is Cloud Computing?

Cloud computing is an emerging technology as it provides services to its users on demand on internet. In this era everybody is using cloud because of its services and the ease which it provides to access those services. In cloud computing it offers different kinds of services to its users on demand over internet on pay per use pattern i.e. the customer needs to pay only that amount which corresponds to its use. In cloud computing it offers different services like sharing of networks, servers, storage, software applications etc. which is required by the users to run their businesses or for their individual work purpose, so they do not need to purchase or acquire any heavy machinery or software, they can use the services which is required by them with the help of cloud service providers, so it becomes very convenient for the users as it reduces the managing cost, maintenance cost as well as purchasing cost of the services which can be a software or any other device which they physically acquire earlier. Although of these positive facts of cloud, there is one major drawback which becomes the obstacle for cloud users to use the services of cloud, i.e. the security of data in cloud, each and every user have some security concern during using cloud services. As in cloud it stores large amount of data of many cloud users and then how it can be assured that data is not accessed by any other user or any intruder so the cloud service seeker might arise the question about the privacy and confidentiality of data, integrity of data, authenticated and authorized access of data, etc. so we can say that data security becomes the major issue in cloud computing.

# International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2015

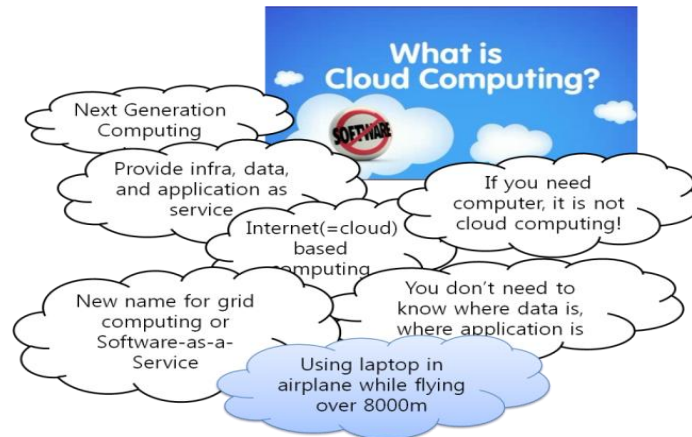


Figure 1: Cloud computing

The above figure 1 describes what cloud computing is in short and brief manner. As in the figure it describes that cloud computing is next generation computing, it provides infrastructure, data and application as service. Moreover it describes that internet is equal to cloud based computing and you don't need to know where data and applications are, and then it shows new name for grid computing is Software as a service.

## DATA SECURITY ISSUES IN CLOUD COMPUTING

Cloud computing is in some way is the base of any small or large size companies, as people are using cloud for running their businesses and in cloud they are sending their data, or using the cloud for data storage purpose, so the major concern of these people is the security of their data i.e. whether their data is secure in cloud or not. So data security becomes the major obstacle in using the services of cloud computing. Some of the key features which can be taken in the context of data security are Data Integrity, Privacy and Confidentiality, Data Availability, Data Location and Relocation, Storage Backup and Recovery.

The figure 2 shows the security in Cloud Computing i.e. it is very important to maintain data security in Cloud Computing. As it describes the security threats and how important to make each and every cloud secure.



Figure 2: Data security in cloud computing

## Data Integrity

Integrity of data means that there should not be any tampering or alteration done to the user data, so to ensure data integrity in cloud environment cloud service provider (CSP) use some effective mechanisms. As user data is very important for them, so to maintain its integrity and be accountable about the data that what happen to data at what point it has to implement some mechanism for data integrity.

# International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2015

## Privacy and Confidentiality

This is the major issue during storing the data in cloud environment, as cloud service provide (CSP) use some mechanism to ensure the privacy and confidentiality of data i.e. the user data should be very confidential and it should not be accessed by anyone else other than the authorized user moreover it should not be accessed by the cloud personnel, so it needs to maintain the privacy and confidentiality of data by using different mechanisms.

## Data Availability

Data availability is another security issue in cloud computing, as cloud service provider (CSP) stores it data in distributed manner i.e. at different locations, so to provide uninterrupted data it needs to use some mechanism.

## Data Location and Relocation

In cloud computing initially it stores data at some place but after sometime it relocates the data i.e. it locate and relocate the data according to the availability and requirement of storage place so in that case it needs to maintain the security of data at different locations.

## Storage, backup and recovery

As we know data is stored in cloud, but what happen if cloud's storage system get corrupted or data theft occur in its storage system, so it needs to use some mechanism to provide the backup and recovery of the lost data.

## RSA Algorithm

The RSA algorithm is the most popular and proven asymmetric key cryptographic algorithm . RSA stands for Ron Rivest, Adi Shamir and Len Adleman, who first publicly described it in 1977. RSA is a block cipher, in which every message is mapped to an integer. RSA consists of Public-Key and Private-Key. Once the data is encrypted with the Public-Key, it can be decrypted with the corresponding Private-Key only.

RSA algorithm involves three steps:

1. Key Generation
2. Encryption
3. Decryption

## Steps

### Key generation

1. Choose two distinct prime numbers  $p$  and  $q$ . For security purposes, the integers  $p$  and  $q$  should be chosen at random and should be of similar bit length.
2. Compute  $N = p * q$ .  $N$  will be used as the module for public key and private key.
3. Select the public key (i.e. the encryption key)  $E$  such that it is not a factor of  $(p-1) * (q-1)$ .
4. Select the private key (i.e. the decryption key)  $D$  such that the following equation is true:  
 $(D * E) \bmod ((p-1) * (q-1)) = 1$ .

### Encryption

5. For Encryption, calculate the cipher text  $CT$  from the plain text  $PT$  as follows:  
 $CT = PT^E \bmod N$ .
6. Send  $CT$  as the cipher text to the receiver.

### Decryption

7. For Decryption, calculate the plain text  $PT$  from the cipher text  $CT$  as follows:  
 $PT = CT^D \bmod N$  [11].

## MD5( Message Digest 5)

MD5 is a message digest algorithm developed by Ron Rivest. MD5 is quite fast and produces 128-bit message digests. After some initial processing, the input text is processed in 512-bit blocks ( which are further divided into 16 32-bit blocks).The output of the algorithm is a set of four 32-bit blocks which make up the 128-bit message digest [11]. It contains various steps which includes Padding, Append length, Divide the input into 512-bit blocks, Initialize chaining variables, and Process blocks.

# International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2015

### One MD5 operation

- A process P is first performed on b, c and d. This process is different in all the four rounds.
- The variable a is added to the output of the process P (i.e. to the register abcd).
- The message sub-block M[i] is added to the output of step2(i.e. to the register abcd).
- The constant t[k] is added to the output of step 3 (i.e. to the register abcd).
- The output of step 4 (i.e. the contents of register abcd) is circular-left shifted by s bits.(The value of s keep changing)
- The variable b is added to the output of step 5 (i.e. to the register abcd).
- The output of step 6 becomes the new abcd for the next step[11].

All the above steps are shown in the following figure 3 i.e. it shows the process of one MD5 operation. As it contains the process P, variables a, b, c, d, message sub-block M[i], constant t[k] for the operation of MD5 algorithm.

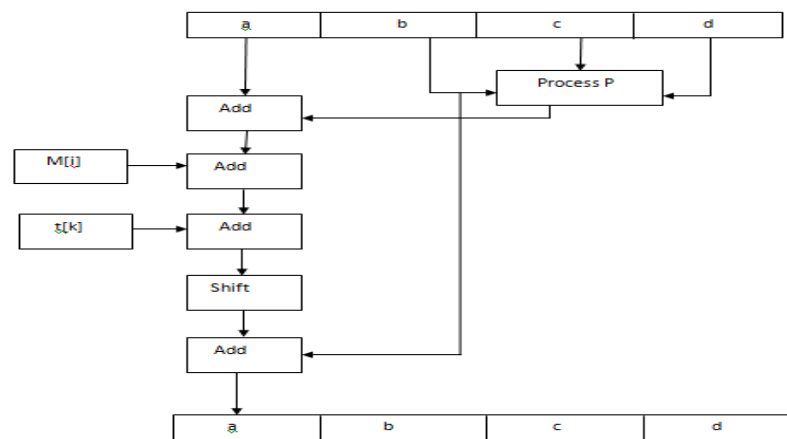


Figure 3: One MD5 operation

We can mathematically express a single MD5 operation as follows:

$$a = b + ((a + \text{Process P}(b, c, d) + M[i] + t[k]) \lll s)$$

where

$\lll s$  = Circular left shift by s bits

### Understanding the process P

As we can see, the most crucial aspect here is to understand the process P, as it is different in the four rounds. In simple terms process P is nothing but some Boolean operations on b, c and d as shown in the following table[11].

Round	Process P
1	(b AND c) OR (( NOT b) AND (d))
2	( b AND d) OR ( c AND ( NOT d))
3	b XOR c XOR d
4	c XOR ( b OR (NOT d))

Table 1: Process P in each round

# International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2015

Above table 1 describes the process of MD5 operation of 4 round, it describes process of each round on Boolean operations using b, c and d. It contains the combination of various Boolean operations like AND, OR, NOT, XOR on the variables b, c and d for the process of all four rounds.

## II. RELATED WORK

Different methods are already implemented to provide the data security in cloud computing. Some authors had tried to use Steganography technique to provide the security of data in cloud. Some other authors applied RSA algorithm for data security in cloud. In this paper we are using RSA algorithm for data security and for maintaining the integrity of key during key transmission we are using MD5 hash generation algorithm and we had also implemented the method for authenticated and authorized access to data, details of the proposed work is given in the next section.

## III. PROPOSED WORK

In our proposed work we are using RSA algorithm for encrypting and decrypting data and MD5 algorithm for generating the hash value of client's public key to maintain the integrity of client's public key during key transmission to the cloud service provider(CSP) as data is encrypted with the help of client's public key by cloud service provider(CSP) and then it is stored in encrypted form in cloud's environment after that the client ask for the data from the cloud service provider (CSP) then after checking the authenticity of the client, cloud service provider(CSP) sends the data to the client after which the client decrypt the data with its own private key and get the original data. We had implemented our work by using MATLAB tool.

Now the step by step process of proposed work is as follows:-

- Key generation will take place on cloud side by using RSA algorithm in which the public key of cloud service provider (CSP) will known to all.
- Key generation takes place on client side by using RSA algorithm in which private key as well as public key both are known to client only and it sent its public key to those whom it want to communicate.
- Client will prepare to send its public key and value of N to cloud service provider (CSP), through which cloud service provider (CSP) will encrypt client's data.
- Client will encrypt its public key and value of N by using cloud service provider (CSP) public key and value of N with the help of encryption process of RSA algorithm, after that a cipher text is generated.
- Client will generate the hash value of cipher text by using MD5 algorithm and then send the cipher text and the hash value to the cloud service provider (CSP).
- After that cloud service provider(CSP) will receive the client message and then generate the hash value for the cipher text by using MD5 algorithm, and then match both the hash values, if both the hash values matches then it accept the message otherwise it discards the message because it indicates the tampering of data.
- After accepting the message cloud service provider (CSP) decrypt the cipher text of client's public key and N by using its own private key and N with the help of RSA algorithm.
- Now, the client (user) send its data to the cloud service provider (CSP) for storing it in its cloud environment or in cloud's database.
- When the cloud service provider (CSP) receives the message or data from the client, then cloud service provider (CSP) encrypts the client's data by using client's public key with help of RSA algorithm and store the client's data in encrypted form in its (cloud's) database.
- After that Client (user) request the cloud service provider(CSP) for its data, so to verify that the request is generated from the authenticated client (user) or not, client (user) encrypts its request by using its (user's) private key with the help of RSA algorithm encryption process and then send it to the cloud service provider (CSP).
- After that cloud service provider (CSP) will decrypt the request by using client's public key with help of RSA algorithm which serves the purpose of authentication and authorization of client (user), because only the client (user) knows its private key, and if it encrypt the request by using its private key then it can only be decrypted by using its corresponding public key.

# International Journal of Innovative Research in Science, Engineering and Technology

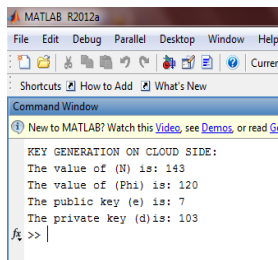
(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2015

- After receiving the request from client (user) to access data , the cloud service provider (CSP) will send the data to the client in encrypted form.
- Then client (user) will decrypt the data by using its private key and get the original data which it requires.

## IV. EXPERIMENTAL RESULTS

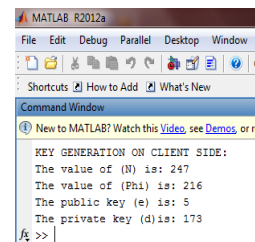
The experimental result of the proposed work is shown in the following figures, as figure 4 and figure 5 shows the key generation on cloud side and client side respectively, firstly it will ask for the prime numbers (p, q) on both sides i.e. the client side and CSP side then it will generate the key on both the sides with the help of RSA algorithm using MATLAB tool.



```

MATLAB R2012a
File Edit Debug Parallel Desktop Window Help
Shortcuts How to Add What's New
Command Window
New to MATLAB? Watch this Video, see Demos, or read Ge
KEY GENERATION ON CLOUD SIDE:
The value of (N) is: 143
The value of (Phi) is: 120
The public key (e) is: 7
The private key (d) is: 103
f1 >>
  
```

Figure 4: Key generation on cloud side



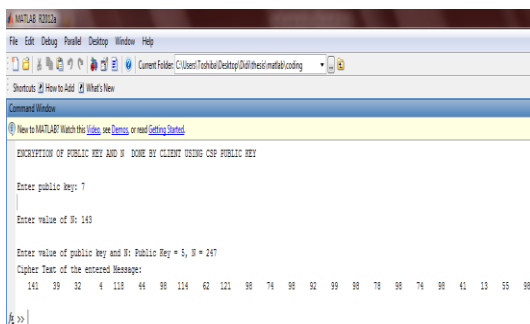
```

MATLAB R2012a
File Edit Debug Parallel Desktop Window Help
Shortcuts How to Add What's New
Command Window
New to MATLAB? Watch this Video, see Demos, or re
KEY GENERATION ON CLIENT SIDE:
The value of (N) is: 247
The value of (Phi) is: 216
The public key (e) is: 5
The private key (d) is: 173
f1 >>
  
```

Figure 5: Key generation on client side

Figure 6 shows the encryption of client’s public key and value of N by using cloud service provider (CSP) public key and N on client side with the help of RSA algorithm this process will take place on client side. Firstly it ask for cloud’s public key and N after that it ask for client’s public key and N and then it encrypts the client’s public and value of N with the help of CSP public key and N.

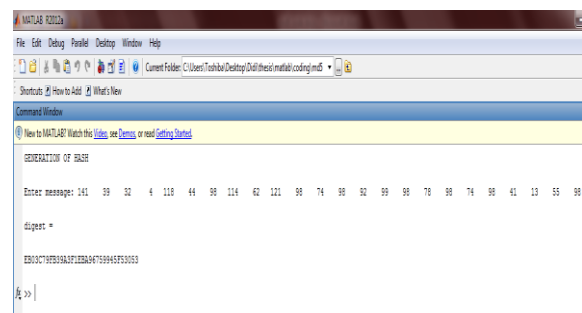
After that figure 7 shows the generation of hash value of the cipher text of client’s public key and N by using MD5 hash generation algorithm to maintain the integrity of public key and N during key transmission this process again takes place on client side. In this firstly it ask for the message to which hash to be generated then it generates the hash value (message digest) for the message and then that hash value is to be sent along with the message to the cloud service provider (CSP) through which CSP can check the tampering of data takes place or not.



```

MATLAB R2012a
File Edit Debug Parallel Desktop Window Help
Shortcuts How to Add What's New
Command Window
New to MATLAB? Watch this Video, see Demos, or read Getting Started
ENCRYPTION OF PUBLIC KEY AND N DONE BY CLIENT USING CSP PUBLIC KEY
Enter public key: 7
Enter value of N: 143
Enter value of public key and N: Public Key = 5, N = 247
Cipher Text of the entered Message:
141 59 32 4 116 44 96 114 62 121 98 74 99 92 99 98 78 98 74 98 41 13 55 98
f1 >>
  
```

Figure 6: Encryption of client’s public key and N



```

MATLAB R2012a
File Edit Debug Parallel Desktop Window Help
Shortcuts How to Add What's New
Command Window
New to MATLAB? Watch this Video, see Demos, or read Getting Started
GENERATION OF HASH
Enter message: 141 59 32 4 116 44 96 114 62 121 98 74 99 92 99 98 78 98 74 98 41 13 55 98
digest =
ED0AC79B59A371E8A46759945F50103
f1 >>
  
```

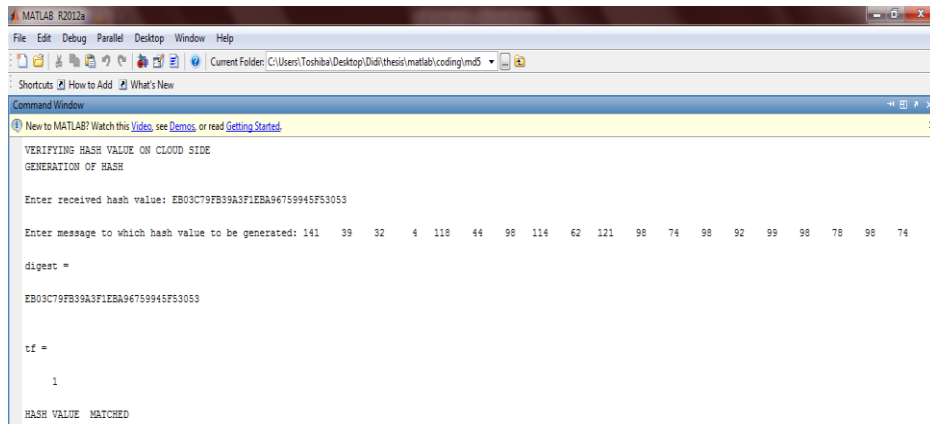
Figure 7: Generation of hash on client side using MD5

Figure 8 shows the verification of hash value on cloud side using MD5 algorithm and again it is implemented in MATLAB. Firstly it ask for the hash value received then it ask for the message which it receives after that it generates the hash value for the message which it receives and then it match both the hash values i.e. it compares both the strings of hash values if the strings matches then it shows the output “HASH VALUE MATCHED” otherwise it shows the output “HASH VALUE DOESN’T MATCHED” which indicates tampering of data takes place in network.

# International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2015



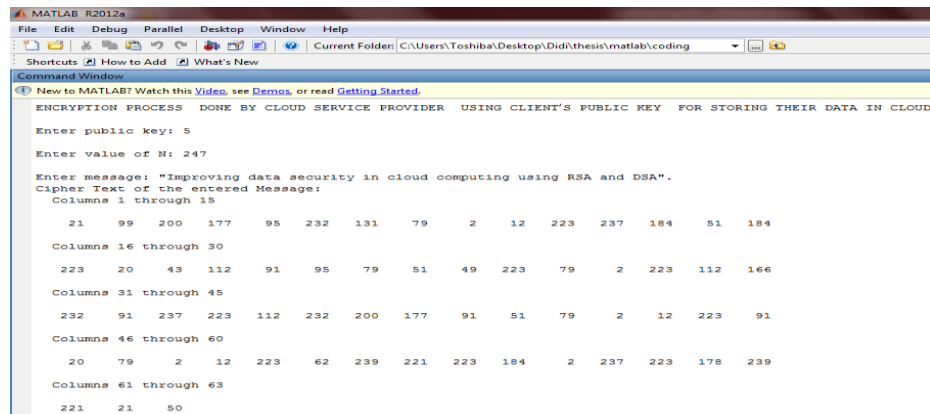
```

MATLAB R2012a
File Edit Debug Parallel Desktop Window Help
Current Folder: C:\Users\Toshiba\Desktop\Did\thesis\matlab\coding\md5
Shortcuts: How to Add What's New
Command Window
New to MATLAB? Watch this Video, see Demos, or read Getting Started.
VERIFICATION HASH VALUE ON CLOUD SIDE
GENERATION OF HASH
Enter received hash value: EB03C79FB9A3F1EBA96759946F53053
Enter message to which hash value to be generated: 141 39 32 4 118 44 98 114 62 121 98 74 98 92 99 98 78 98 74 9
digest =
EB03C79FB9A3F1EBA96759946F53053
tf =
1
HASH VALUE MATCHED

```

Figure 8: Verification of hash value on cloud side.

Now Figure 9 shows the encryption of client's data done by cloud service provider (CSP) by using client's public key and N with the help of RSA algorithm and after that the cloud service provider (CSP) stores the client's data in encrypted form. In this firstly CSP ask for the client's public key and value of N which it receives from client after that it ask for the message which it receives from the client then it encrypts the client message with the help of client's public key and store the data in cloud's database in encrypted form.



```

MATLAB R2012a
File Edit Debug Parallel Desktop Window Help
Current Folder: C:\Users\Toshiba\Desktop\Did\thesis\matlab\coding
Shortcuts: How to Add What's New
Command Window
New to MATLAB? Watch this Video, see Demos, or read Getting Started.
ENCRYPTION PROCESS DONE BY CLOUD SERVICE PROVIDER USING CLIENT'S PUBLIC KEY FOR STORING THEIR DATA IN CLOUD
Enter public key: 5
Enter value of N: 247
Enter message: "Improving data security in cloud computing using RSA and DSA".
Cipher Text of the entered Message:
Columns 1 through 15
21 99 200 177 95 232 131 79 2 12 223 237 184 51 184
Columns 16 through 30
223 20 43 112 91 95 79 51 49 223 79 2 223 112 166
Columns 31 through 45
232 91 237 223 112 232 200 177 91 51 79 2 12 223 91
Columns 46 through 60
20 79 2 12 223 62 239 221 223 184 2 237 223 178 239
Columns 61 through 63
221 21 50

```

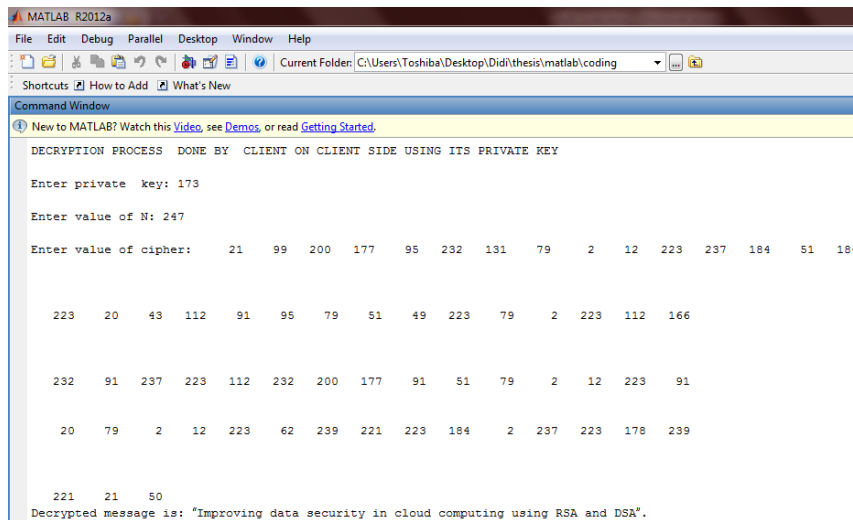
Figure 9: Encryption of message on cloud side using client's public key.

Figure 10 shows the decryption of client's data done by client using its private key with help of RSA algorithm, as client ask CSP for its data then the CSP check the authenticity of the client and then send the data in encrypted form to the client and then client will decrypt the data using its private key and get the original data. In this the client will enter its private key and value of N and then it enters the received cipher text (message in encrypted form) after that it decrypts the cipher text by using its private key and value of N with the help of RSA algorithm and get the original data which it requires.

# International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2015



```

MATLAB R2012a
File Edit Debug Parallel Desktop Window Help
Current Folder: C:\Users\Toshiba\Desktop\Didi\thesis\matlab\coding
Command Window
New to MATLAB? Watch this Video, see Demos, or read Getting Started.
DECRYPTION PROCESS DONE BY CLIENT ON CLIENT SIDE USING ITS PRIVATE KEY

Enter private key: 173

Enter value of N: 247

Enter value of cipher: 21 99 200 177 95 232 131 79 2 12 223 237 184 51 184

223 20 43 112 91 95 79 51 49 223 79 2 223 112 166

232 91 237 223 112 232 200 177 91 51 79 2 12 223 91

20 79 2 12 223 62 239 221 223 184 2 237 223 178 239

221 21 50

Decrypted message is: "Improving data security in cloud computing using RSA and DSA".
  
```

Figure 10: Decryption of message on client side using client's private key.

## V. CONCLUSION

As we all know, data security is the most important paradigm in each and every field of web, so it is in cloud computing, hence in our proposed work we are working for the security of data and maintaining the integrity of public key during key transmission by using RSA algorithm and MD5 hash generation algorithm respectively through which we meet the objectives of privacy and confidentiality of data, integrity of data, authenticated and authorized access to the data. In the end we can say that cloud computing is still an evolving technology so it requires many modifications regarding its security issues.

## REFERENCES

- [1] Parsi Kalpana ,Sudha Singaraju, "Data Security in Cloud Computing using RSA Algorithm" International Journal of Research in Computer and Communication technology, IJRCCT, ISSN 2278-5841, Vol 1, Issue 4, September 2012.
- [2] Allan A. Friedman and Darrell M. West, "Privacy and Security in Cloud Computing" Issues in technology innovation, number 3 (2010).
- [3] Vahid Ashktorab2, Seyed Reza Taghizadeh1, "Security Threats and Countermeasures in Cloud Computing" International Journal of Application or Innovation in Engineering & Management (IJAIEM) Volume 1, Issue 2, October 2012 ISSN 2319 – 4847.
- [4] Rajesh Piplode, " An Overview and Study of Security Issues & Challenges in Cloud Computing" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 9, September 2012 ISSN: 2277 128X.
- [5] Rabi Prasad Padhy, "Cloud Computing: Security Issues and Research Challenges " IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS) Vol. 1, No. 2, December 2011.
- [6] Shreya Srivastav, Shalika "Improving data security in cloud computing by using RSA and Digital Signature Algorithm "A special issue of IJTR(ISSN 2278-5787) SERB sponsored two day national conference on " Current trends in scientific research for engineering applications (NCCSE-2015)" dated march 20-21, 2015.
- [7]R.L. Rivest, A. Shamir, and L. Adleman "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems" developed in 1977.
- [8] Amare Anagaw Ayele, Dr. Vuda Sreenivasarao "A Modified RSA Encryption Technique Based on Multiple public keys" International Journal of Innovative Research in Computer and Communication Engineering, Vol. 1, Issue 4, June 2013.
- [9] Erfaneh Noroozi, Salwani Mohd Daud, Ali Sabouhi " Secure Digital Signature Schemes Based on Hash Functions" International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-2, Issue-4, March 2013.
- [10] Priyanka Walia, Vivek Thapar "Implementation of New Modified MD5-512 bit Algorithm for Cryptography" International Journal of Innovative Research in Advanced Engineering (IJIRAE) ISSN: 2349-2163 Volume 1 Issue 6 (July 2014).
- [11] Atul Kahate "Cryptography and Network Security".
- [12] Chetan S. Kadu, Abhay A. Jadhav, Prashant L. Mandale "Improving Security of Cloud Environment in Dynamic Cloud Network" (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (2) , 2014, 1681-1684.