Performance Analysis of mRSA for Varying Key Sizes and Data Modulus

Manvi goyal [#1], Jatin Sharma [*2]
[#1]*M.Tech. Student,* [*2]*Assistant Professor, Department of CSE,*
Rawal institute of Engineering and technology, M.D. University, Rohtak, Haryana, India

Abstract

As all we know that we depend on internet, because everything is going to be shifted on internet. Because internet is one of the way from where we can share any information globally. As Mostly organizations or any enterprise shift their data on internet to access their data from anywhere. Now, in this modern era there is a new technology which is named as cloud computing is used. Cloud computing doesn't required any hardware devices and storage devices but we have an internet connection So it can be used by an Enterprises or an organization to access data from anywhere. Cloud computing gained importance because it reduced the cost of storage and processing, growth technologies of visualization. In this paper we describe the security issues of cloud computing i.e. we analyze the time of encryption and decryption by sending messages. Before analyzing this issue, we discuss definition of cloud computing, then its characteristics. Then we discuss various models of cloud computing, platforms and some other things and give some solution for security issues.

Keywords —*Service models, computing services, identity based encryption, mediated RSA*

I. INTRODUCTION

In cloud computing the word cloud is used as a metaphor for the "Internet" .It is a type of internet based computing where different services such as storage, servers, application etc. are provided to the computer which are used in any organizations and also to the devices.

Cloud computing is on the most valuable technology and mostly everyone talked about this technology. As all we know that whole data of every enterprise is shifted on internet so that it can be accessed from anywhere but it requires hardware devices, storage devices and an internet connection. But now Cloud computing has a great importance in enterprises, and whole data of enterprise is shifted on internet as we know so that anyone can access the data from anywhere without the need of hardware devices and storage devices but need an internet connection to access the data. CLOUD means common location independent online utility on demand. Cloud computing is defined as" cloud computing means storing and accessing programs and data over the internet instead of yours computer's hard drive. Cloud technology is increasing day by day and now it is beneficial for small and large industries. Companies providing virtualized environment by which it omits the needs for physical storage and others like Microsoft, Amazon etc.

Certain algorithms like RSA, DSA, Ceaser Cipher etc. to improve the security issues of cloud Computing. And we can say that Cloud Computing will become most popular in the next few years or it will be a future in the next years. Possibly, everyone will find everything on their desktop. Cloud computing provide computing related IT capabilities by which user can get any information which they want at any time. Cloud Computing will become the future for industries.

The Cloud Computing should have concept is that we should have an internet connection, storage devices and does not need any hardware devices. If we take the example of email say Yahoo, Gmail, Hotmail these take cares of all the necessary hardware and software needed for the user to support their applications. We can access our email from anywhere from we want in the same way in cloud computing our data is stored on the cloud and we can access it whenever we have any need and We can access in any source like in desktop, mobile phones or in tablets is one of the major advantage.

A. Motivation

In Traditional system, certain algorithms are applied to improve the security of the data e.g. RSA, DES and other symmetric and asymmetric algorithms. In Identity based encryption algorithm it also finds out the encryption and decryption time but there is a basic problem of Key Escrow.

On the other hand there is mediated RSA which split the RSA private key between user and SEM. And by combining these two (IBE and mRSA) we found out encryption and decryption time on small key size. This mainly led us to focus our project on variable key size on specific modulus.

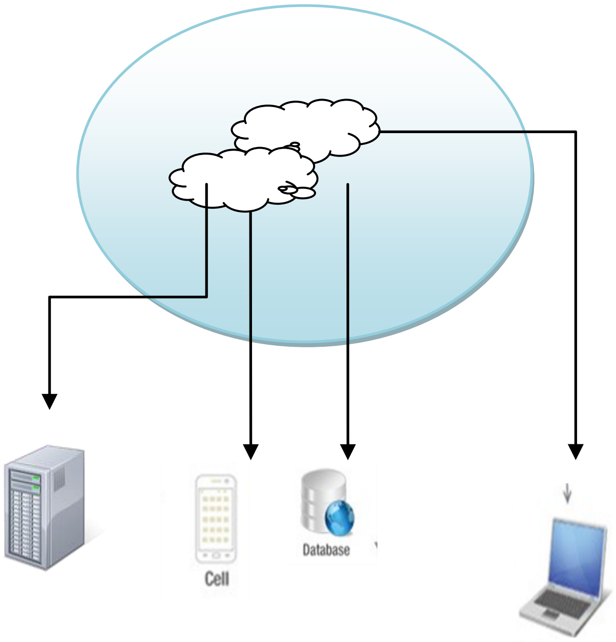


Fig – 1 Area of Cloud Computing

B. *Characteristics of Cloud computing*

1) Multi-tenancy

Multi-tenancy – it means multiple tenants at the same instant. This allows sharing the infrastructure between several customers without being aware of sharing to each other. . The developer should not compromise with the privacy of the data of users. This is done by virtualizing the servers on machine pool and then it allots the server to the requested customers.

2) Linearly Scalable

Linearly scalable in which workload can be divide between different infrastructures. For example if one server can process 500 transactions at one time then two server can process 1000 transactions at one time and so on. System here broke down the workload and service. The idea of scalability obtained from the fact that a server is able to process many transactions at one time.

3) Service-oriented

One of the main feature of cloud computing is that they are service oriented it means that many computing services are different computing services are combined with each other. The main advantage of this method is we can reuse many services. It offers many independent services to combine together so that the users need can be fulfilled at their demand. One of the other advantage of this method is cost can be minimized by some companies because many companies combine with each other services.

4) Virtualized

Virtualization of data makes data separate from the user's side. The cloud data is not available to the user because they are stored on the server side and user is not available to see it. Whenever user put any demand of any data on their system then this data make available to the customers by picking the data from the cloud servers. Cloud computing provide computing related IT capabilities by which user can get any information which they want at any time. Cloud Computing will become the future for industries. The Cloud Computing should have concept is that we should have an internet connection, storage devices and does not need any hardware devices. It is one of the major advantages.

C. *Aims and Objective*

In this modern era, cloud computing is increasing day by day but its threats are also increasing. The main aim of this research is to analyse the performance of Identity based Cryptography with mRSA for variable key size in respect to the time taken for encryption and decryption. In this report, we have use modulus i.e. 512 bits, 1024 bits, 2048 bits on which we use these variable key size i.e 512 bits, 1024 bits, 2048 bits on each modulus to find out encryption and decryption time.

D. *Problem Statement*

With increase of in use, clouds are prone more towards security attacks. If we use large bit size message then this required more security because there are more chances of security attacks if we increase key size. So by using Identity Based encryption with mediated RSA we find out the encryption time and decryption time by which we will see that how is time changing. By seeing that we reduce the security attacks.

II. SERVICE MODELS

Basically cloud is divided into two parts:

1. Front end – It includes user and customer
2. Back end - It includes collection of various hardware devices like RAM, Hard disk etc.

Apart from back end and front end we also have an Administrator whose work is to check "Is everything going smoothly or not". It follows some set of rules which are called Protocols and use a special kind of software called Middle ware.

Cloud computing has three service models which are:-

1. Public Cloud
2. Private Cloud
3. Hybrid Cloud

Public Cloud :- . Public clouds are accessible to anybody. In daily life we access certain applications like Google, Yahoo etc. are example of public cloud.

Public clouds are not so much secure as compared to private clouds because here any third party can access the data because they are available openly. There is no security concerns in public cloud This model is also explains the pay per user model in which user is able to access the data which he have demanded.

Benefits:-

- The Cost investment is low because user have to pay for what he want to use.
- It is good for large server and large scale data.

Private Cloud :- Private cloud is company's own data centre where the employers of companies can access the data and store this data. It is easier to regulate the data in private cloud because it is limited only with the organization. Security is better in private cloud as compared to other model. There is a main difference between private and public cloud is that the private cloud in which security is well maintained within the organization because no other third party can access the data of organization without permission of the organization.

Benefits:-

- Now IT firms have their control on the access of data
- Security concerns are reduced as all data can be managed in only one place.

Hybrid Cloud:- Hybrid cloud are both combination of public and private cloud as they combine features of both the clouds. It combines feature of virtualization environment as provided in private cloud and they also use of public model which use traditional computers but they should have hard disk, internet and other means to access the data. It provides more security to data because it combines features of both the clouds. It also give more access of data to the customer. For virtualizing environment companies should have physical servers, routers, sockets and many others. For accessing the data virtually internet connection and computers must be required with users.

Benefits :-

- Operational flexibility: run critical mission on private cloud
- Scalability: It should be capable to run with lots of data.

Community cloud:- There are many organizations who have same interest and requirement of data. This need of sharing data can be shared between different organizations. This operation can be within the company or outside the company also. Companies with same interest can save lots of money by sharing. This model is very helpful for small IT companies and business.

Benefits:-

- Very economical for small companies
- Different organizations can shared their data with each other.

1) Computing Services

The security consideration relates to the various cloud computing service delivery models. The three main cloud service delivery models are:

a) Infrastructure as a Service (IaaS)
b) Platform As a Service (PaaS)
c) Software As A Service (SaaS)

(a) Software as a Service (SaaS):

SaaS is the model which can be accessed from the internet by the users. Customers have no need of, purchasing software licenses, while the expenses are lowered for the cloud services providers, since only some application needs to be hosted and maintained. Thus SaaS eliminates customer fears about application servers, application development, storage and related common concerns of IT firms. Some examples are Salesforce.com, Google's Gmail & Apps, Yahoo and Google, and VoIP from Vonage and Skype and Microsoft, Zoho, etc.

It can be divided into two categories:

- **Line of Business Service**
- **Customer-oriented Service**

Characteristics of SaaS

Some of the characteristics of SaaS include following properties:-

•Web access to commercial software.
•Software is managed from a central location.

(b) Platform as a Service (PaaS):

PaaS provides virtualized servers where users can run applications, or they can also develop new ones, without having worry about maintaining the operating systems, server hardware, load balancing, computing capacity and many others. LAMP platform (Linux, Apache, MySQL and PHP), restricted J2EE, are some of the popular PaaS examples which meet the scalability requirements of the applications.

a) ***Development facilities:*** This allow existing applications to be customized. The add-on development facilities allow users to enhance the feature of SaaS applications

b) ***Stand-alone environments:*** These environments do not include licensing, technical dependencies for general developments. Application delivery-only environments These environments supports hosting level services like security and on demand scalability. It reduces greenhouse effect by the utilization of vacant resources of computer to increase the efficiency through improving utilization rate and reduce energy.

Characteristics of PaaS

Some of the basic characteristics include following:-

•Services can be developed, deploy, host, test and maintain applications in same development environment.

•Multi-tenant architecture means many users use the same applications like which are used in community development.

• The Scalability feature of cloud computing includes load balancing and fail over.

(c) Infrastructure as a Service (IaaS):

IaaS means infrastructure as a service and it provides basic storage functions , computing capabilities as standardized services over the network. A typical way to implement such a system is platform virtualization, where the user of the system can consider that the service corresponds to a piece of hardware and associated system software Servers, networking equipment, storage systems and data centre space etc. are collected together and they are made available to handle heavy workloads. The IaaS customer can rent computing resources and they have no need of buying and installing them on their own data centre. The service also based on the pay per model basis. What is done if a costumer required more resources? Here the services include dynamic scaling so if a customer needs more resources he can get these resources immediately. Dynamic scaling applied means that the infrastructure automatically managed their resources based on the requirement of the customers.

Characteristics of IaaS:-

If we compared the two models of IaaS and PaaS, we can say that the IaaS model is rapidly developing. Some core characteristics describe what actually IaaS is. IaaS is generally have following characteristics:-

• Resources are easily available to the customers on demand.

• It has a low pricing utility

• It allow for dynamic scaling.

III. PROPOSED WORK AND ALGORITHM

We have proposed the identity based Encryption with Mediated RSA. The advantage of using this approach to provide better security in Software as a Service Model (SaaS). IBE-mRSA will provide integrity and confidentiality to the communication system in SaaS Cloud.It is based on Public Key Encryption algorithm Mediated RSA and Basic Identity Based Cryptography scheme. This IBE-mRSA scheme uses bilinear mapping of two large prime numbers from the two sets of prime numbers. It has also four functions

- **Setup** : generates global parameters and a master key
- **Key generator** : uses the master key to generate private key from public key ID string.
- **Encryption** : generates cipher using public key ID.
- **Decryption** : decodes cipher using the private key.

IBE WITH MEDIATED RSA : PROPOSED ALGORITHM

1. Setup(ID_r)

Input: Identity of Receiver.

Method:

1. Take random s $\in \mathbb{Z}_q^*$, which is master key of prime order q.
2. Public Key P_{id} is defined as

$$P_{id} = s \bullet H(ID_r)$$

Output: Public Key P_{id}

2. Keygen(P_{id})

Input: Public Key P_{id}

Method:

1. Let k be the security parameter
2. Generate random k/2-bit primes, p′ and q′
   such that p = 2p′ + 1 and q = 2q′ + 1.
   are also prime.
3. n ← pq, e $\in_R \mathbb{Z}_{\emptyset(n)}^*$, such that
   $d \leftarrow e^{-1} \bmod \emptyset(n)$
4. For each user (x)
   a. $s \leftarrow k - | P_{id} | - 1$
   b. $e_x \leftarrow 0^s \| P_{id} \| 1$
   c. $d_x \leftarrow 1 / e_x \bmod \emptyset(n)$
   d. $d_{x,u} \leftarrow Z_n \oplus 1 - \{0\}$ //private key for user
   e. $d_{x,sem} \leftarrow (d - d_{x,u}) \bmod \emptyset(n)$ //private key for SEM

Output: Private key for user and Security Mediator,
security parameter, modulus n.

3. Encryption(k, P_{id}, n)

Input: Public Key P_{id}, Security Parameter k and

```
        Modulus n
    Method:
        1. Retrieve $P_{id}$ from Setup procedure.
        2. $s \leftarrow k - |P_{id}| - 8$
        3. $e \leftarrow 0^s \| P_{id} \| 1$
        4. Encrypt message m with (e, n) using standard RSA technique.
    Output: Encrypted Message m′.
```

4. Decryption(m′)

```
 Input: Encrypted Message
    Method:
        1. User m′ = encrypted message
        2. User sends m′ to SEM
        3. In parallel,
             SEM:
                 1. If USER revoked return (ERROR)
                 2. $PD_{sem} \leftarrow m'^{\,dsem} \bmod n$
                 3. Send $PD_{sem}$ to USER
             USER:
                 4. $PD_u \leftarrow m'^{du} \bmod n$
        4. USER: $M \leftarrow (PD_{sem} * PD_u) \bmod n$
        5. USER: If succeed, return (m)
```

IV. IMPLEMENTATION

We use ubuntu software to implement this software, which is an open source software of Linux. We can run this in other software of Linux.

The proposed system is implemented using OpenSSL library, Socket Programming and C language. In which first Sender sends a request by sending ID of Receiver to generate public key and private key to Key Generation Centre (KGC). Here, KGC is receiving request for key generation. That will generate key from the ID of Receiver. Here experiment is exercised for the key size of 512 bits, 1024 bits, 2048 bits on specific modulus.Some steps are as:

Step :1 Installation of Ubuntu operating system on desktop:

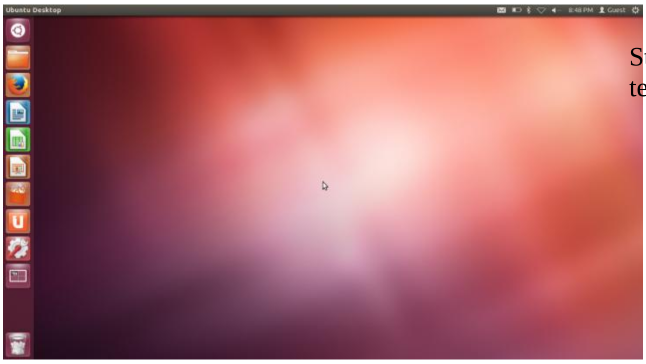
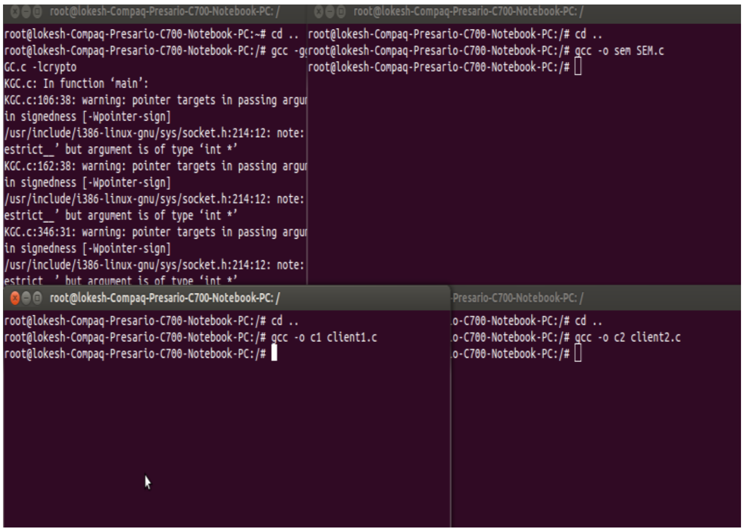


Figure 2: Desktop Page

Step 2: Open 4 terminal and run these commands:



```
root@lokesh-Compaq-Presario-C700-Notebook-PC:~# cd ..
root@lokesh-Compaq-Presario-C700-Notebook-PC:/# gcc -g
GC.c -lcrypto
KGC.c: In function ‘main’:
KGC.c:106:38: warning: pointer targets in passing argu
in signedness [-Wpointer-sign]
/usr/include/i386-linux-gnu/sys/socket.h:214:12: note:
estrict__’ but argument is of type ‘int *’
KGC.c:162:38: warning: pointer targets in passing argu
in signedness [-Wpointer-sign]
/usr/include/i386-linux-gnu/sys/socket.h:214:12: note:
estrict__’ but argument is of type ‘int *’
KGC.c:346:31: warning: pointer targets in passing argu
in signedness [-Wpointer-sign]
/usr/include/i386-linux-gnu/sys/socket.h:214:12: note:
estrict__’ but argument is of type ‘int *’
```

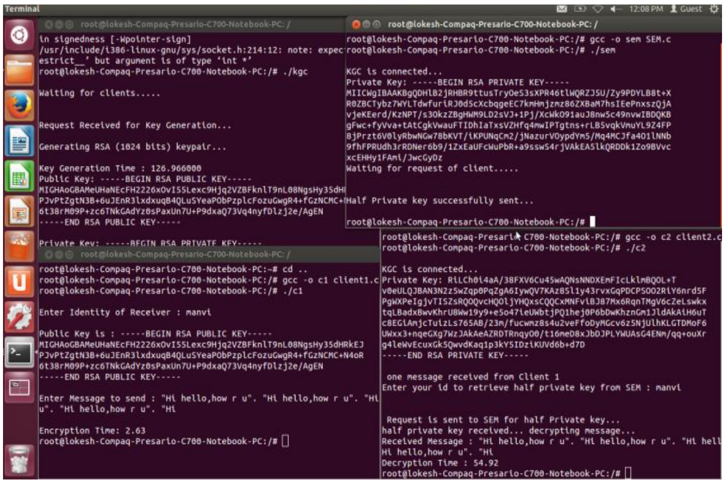
```
root@lokesh-Compaq-Presario-C700-Notebook-PC:/# cd ..
root@lokesh-Compaq-Presario-C700-Notebook-PC:/# gcc -o sem SEM.c
root@lokesh-Compaq-Presario-C700-Notebook-PC:/#
```

```
root@lokesh-Compaq-Presario-C700-Notebook-PC:/# cd ..
root@lokesh-Compaq-Presario-C700-Notebook-PC:/# gcc -o c1 client1.c
root@lokesh-Compaq-Presario-C700-Notebook-PC:/#
```

```
o-C700-Notebook-PC:/# cd ..
o-C700-Notebook-PC:/# gcc -o c2 client2.c
o-C700-Notebook-PC:/#
```

Figure 3: Run commands on 4 terminals

Step 3: Run all other commands in other three terminals for 1024 bits on 512 modulus:-



```
in signedness [-Wpointer-sign]
/usr/include/i386-linux-gnu/sys/socket.h:214:12: note: expec
estrict__’ but argument is of type ‘int *’
root@lokesh-Compaq-Presario-C700-Notebook-PC:/# ./kgc

Waiting for clients.....


Request Received for Key Generation...

Generating RSA (1024 bits) keypair...

Key Generation Time : 126.966000
Public Key: -----BEGIN RSA PUBLIC KEY-----
MIGHAoGBAMeUHaNEcFH2226xOvI55Lexc9Hjq2VZBFknlT9nL08NgsHy35dH
PJvPtZgtN3B+6uJEnR3lxdxuqB4QLuSYeaPObPzplcFozuGwgR4+fGzNCMC+
6t38rM09P+zc6TNkGAdYz0sPaxUn7U+P9dxaQ73Vq4nyfDlzj2e/AgEN
-----END RSA PUBLIC KEY-----

Private Key: -----BEGIN RSA PRIVATE KEY-----
```

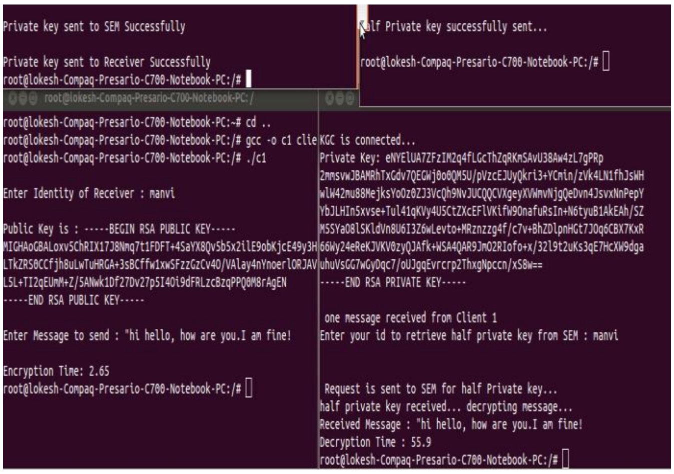
```
root@lokesh-Compaq-Presario-C700-Notebook-PC:/# gcc -o sem SEM.c
root@lokesh-Compaq-Presario-C700-Notebook-PC:/# ./sem

KGC is connected...
Private Key: -----BEGIN RSA PRIVATE KEY-----
MIICWgIBAAKBgQDHlB2jRHBR9ttusTryOeS3sXPR46tlWQRZJ5U/Zy9PDYLB8t+X
R0ZBCTybz7WYLTdwfuriRJ0d5cXcbqgeEC7kmHmjzmz86ZXBaM7hsIEePnxszQjA
vjeKEerd/KzNPT/s3OkzZBgHWM9LD2sVJ+1Pj/XcWkO91auJ8nw5c49nvwIBDQKB
gFwc+fyVva+tAtCgkVwauFTIDhIaTxsVZHfq4mwIPTgtns+rLB5vqkVmuYL9Z4FP
8jPrzt6V0lyRbwNGw78bKVT/iKPUNqCm2/jNazurVOypdYm5/Mq4MCJfa4O1lNNb
9fhFPRUdh3rRDNer6b9/1ZxEaUFcWuPbR+a9ssw54rjVAkEA5lkQRDDk1Zo9BVvc
xcEHHy1FAmi/JwcGyDz
Waiting for request of client.....


Half Private key successfully sent...

root@lokesh-Compaq-Presario-C700-Notebook-PC:/#
```

```
root@lokesh-Compaq-Presario-C700-Notebook-PC:~# cd ..
root@lokesh-Compaq-Presario-C700-Notebook-PC:/# gcc -o c1 client1.c
root@lokesh-Compaq-Presario-C700-Notebook-PC:/# ./c1

Enter Identity of Receiver : manvi

Public Key is : -----BEGIN RSA PUBLIC KEY-----
MIGHAoGBAMeUHaNEcFH2226xOvI55Lexc9Hjq2VZBFknlT9nL08NgsHy35dHRkEJ
PJvPtZgtN3B+6uJEnR3lxdxuqB4QLuSYeaPObPzplcFozuGwgR4+fGzNCMC+N4oR
6t38rM09P+zc6TNkGAdYz0sPaxUn7U+P9dxaQ73Vq4nyfDlzj2e/AgEN
-----END RSA PUBLIC KEY-----

Enter Message to send : "Hi hello,how r u". "Hi hello,how r u". "Hi
u". "Hi hello,how r u". "Hi

Encryption Time: 2.63
root@lokesh-Compaq-Presario-C700-Notebook-PC:/#
```

```
root@lokesh-Compaq-Presario-C700-Notebook-PC:/# gcc -o c2 client2.c
root@lokesh-Compaq-Presario-C700-Notebook-PC:/# ./c2

KGC is connected...
Private Key: RiLCh0i4aA/38FXV6Cu45wAQNsNNDXEmFIcLklmBQOL+T
v0eULQJBAN3N2z5wZqp0PqZgA6IywQV7KAz8Sl1y43rvxGqPDCPSOO2RiY6nrd5F
PgWXPeIgjvTISZsRQOQvcHQOljYHQxsCQQCxMNFviBJ87Mx6RqnTMgV6cZeLswkx
tqLBadxBwvKhrU8Ww19y9+e5o47ieUWbtjPQ1hej0P6bDwKhznGm1JldAkAiH6uT
c8EGiAmjcTuizLs765AB/23m/fucwmz8s4u2veFfoDyMGcv6z5NjUlhKLGTDMoF6
UWxx3+nqeGXg7WzJAkAeAZRDTRnqyO0/t16meD8xJbDJPLYWUAsG4ENm/qq+ouXr
g4leWvEcuxGk5QwvdKaq1p3kY5IDziKUVd6b+d7D
-----END RSA PRIVATE KEY-----

 one message received from Client 1
Enter your id to retrieve half private key from SEM : manvi


 Request is sent to SEM for half Private key...
half private key received... decrypting message...
Received Message : "Hi hello,how r u". "Hi hello,how r u". "Hi hell
Hi hello,how r u". "Hi
Decryption Time : 54.92
root@lokesh-Compaq-Presario-C700-Notebook-PC:/#
```

Figure 4: Commands in other three terminals for 1024 bits on 512 Modulus

Step 4: Run all other commands in other three terminals for 1024 bits on 1024 modulus:-



```
Private key sent to SEM Successfully

Private key sent to Receiver Successfully
root@lokesh-Compaq-Presario-C700-Notebook-PC:/#
```

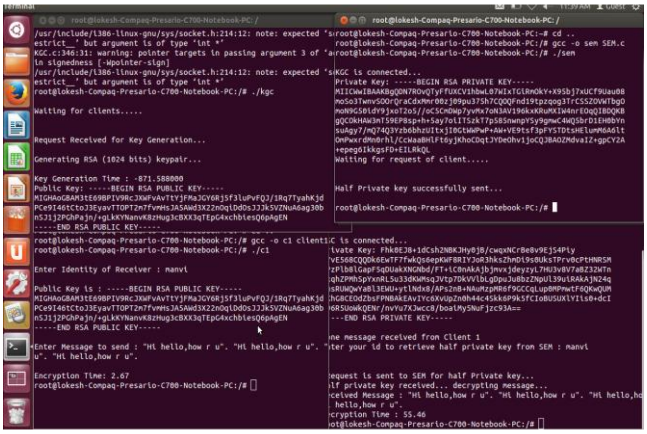
```
Half Private key successfully sent...

root@lokesh-Compaq-Presario-C700-Notebook-PC:/#
```

```
root@lokesh-Compaq-Presario-C700-Notebook-PC:~# cd ..
root@lokesh-Compaq-Presario-C700-Notebook-PC:/# gcc -o c1 clie
root@lokesh-Compaq-Presario-C700-Notebook-PC:/# ./c1

Enter Identity of Receiver : manvi

Public Key is : -----BEGIN RSA PUBLIC KEY-----
MIGHAoGBALoxv5ChRIX17J8Nmq7t1FDFT+4SaYX8Qv5b5x2ilE9obKjcE49y3H
LTkZRS0CCfjh8uLwTuHRGA+3sBCffw1xwSFzzGzCv40/VAlay4nYnoerlORJAV
L5L+TI2qEUmM+Z/5ANwk1Df27Dv27p5I40i9dFRLzcBzqPPQ0M8rAgEN
-----END RSA PUBLIC KEY-----

Enter Message to send : "hi hello, how are you.I am fine!

Encryption Time: 2.65
root@lokesh-Compaq-Presario-C700-Notebook-PC:/#
```

```
KGC is connected...
Private Key: eNYElUA7ZFzIM2q4fLGcThZqRKmSAvU38Aw4zL7gPRp
2mmsvwJBAMRhTxGdv7QEGWj0o0QM5U/pVzcEJUyQkri3+YCmin/zVk4LN1fhJsWH
wlW42mu88MejksYoOz0ZJ3VcQh9NvJUCQQCVXgeyXVWmvNjgQeDvn4JsvxNnPepY
YbJLHIn5xvse+Tul41qKVy4U5CtZXcEFlVKifW9OnafuRsIn+N6tyuB1AkEAh/SZ
M5SYaO8lSKldVn8U6I3Z6wLevto+MRznzzg4f/c7v+BhZDlpnHGt7JOq6CBX7KxR
66Wy24eReKJVKV0zyQJAfk+WSA4QAR9JmO2RIofo+x/32l9t2uKs3qE7HcXW9dga
uhuVsGG7wGyDqc7/oUJgqEvrcrp2ThxgNpccn/xS8w==
-----END RSA PRIVATE KEY-----

 one message received from Client 1
Enter your id to retrieve half private key from SEM : manvi


 Request is sent to SEM for half Private key...
half private key received... decrypting message...
Received Message : "hi hello, how are you.I am fine!
Decryption Time : 55.9
root@lokesh-Compaq-Presario-C700-Notebook-PC:/#
```

Figure 5: Commands in other three terminals for 1024 bits on 1024 Modulus

Step 4: Run all other commands in other three terminals for 1024 bits on 2048 modulus:-



```
/usr/include/i386-linux-gnu/sys/socket.h:214:12: note: expected 's
estrict__' but argument is of type 'int *'
KGC.c:346:31: warning: pointer targets in passing argument 3 of 'a
in signedness [-Wpointer-sign]
/usr/include/i386-linux-gnu/sys/socket.h:214:12: note: expected 's
estrict__' but argument is of type 'int *'
root@lokesh-Compaq-Presario-C700-Notebook-PC:/# ./kgc

Waiting for clients.....


Request Received for Key Generation...

Generating RSA (1024 bits) keypair...

Key Generation Time : -871.588000
Public Key: -----BEGIN RSA PUBLIC KEY-----
MIGHAoGBAM3tE69BPIV9RcJXWFvAvTtYjFMaJGY6Rj5f3luPvFQJ/1Rq7TyahKjd
PCe9I46tCtoJ3EyavTTOPT2m7fvmHsJA5AWd3X22nOqiDdOsJJJk5VZNuA6ag30b
nSJ1j2PGhPajn/+gLkKYNanvK8zHug3cBXX3qTEpG4xchbiesQ6pAgEN
-----END RSA PUBLIC KEY-----
```

```
root@lokesh-Compaq-Presario-C700-Notebook-PC:~# cd ..
root@lokesh-Compaq-Presario-C700-Notebook-PC:/# gcc -o sem SEM.c
root@lokesh-Compaq-Presario-C700-Notebook-PC:/# ./sem

KGC is connected...
Private Key: -----BEGIN RSA PRIVATE KEY-----
MIICWwIBAAKBgQDN7ROvQTyFfUXCV1hbwL07WIxTGiRmOkY+X95bj7xUCf9Uau08
moSo3TwnvSOOrQraCdxMmr00zj09pu37Sh7CQOQFnd19tpzqog3TrCSSZOVWTbgO
moN9G50idY9jxoT2o5//oC5CmDWp7yvMx7oN3AV196kxKRuMXIW4nrEOqQIBDQKB
gQCOkHAW3mT59EP8sp+h+Say7oiITSzkT7p5B5nwnpYSy9gmwC4WQ5brD1EH0bYn
suAgy7/mQ74Q3Yzb6bhzUItxjI0GtWWPwP+AW+VE9tsf3pFYSTDtsHElumM6A6lt
OmPwxrdMn0rhl/CcWaaBHlFt6yjKhoCDqtJYDeOhv1joCQJBAOZMdvaIZ+gpCY2A
+epeg6IkkgsFD+EILRkQL
Waiting for request of client.....


Half Private key successfully sent...

root@lokesh-Compaq-Presario-C700-Notebook-PC:/#
```

```
root@lokesh-Compaq-Presario-C700-Notebook-PC:/# gcc -o c1 client1
root@lokesh-Compaq-Presario-C700-Notebook-PC:/# ./c1

Enter Identity of Receiver : manvi

Public Key is : -----BEGIN RSA PUBLIC KEY-----
MIGHAoGBAM3tE69BPIV9RcJXWFvAvTtYjFMaJGY6Rj5f3luPvFQJ/1Rq7TyahKjd
PCe9I46tCtoJ3EyavTTOPT2m7fvmHsJA5AWd3X22nOqiDdOsJJJk5VZNuA6ag30b
nSJ1j2PGhPajn/+gLkKYNanvK8zHug3cBXX3qTEpG4xchbiesQ6pAgEN
-----END RSA PUBLIC KEY-----

Enter Message to send : "Hi hello,how r u". "Hi hello,how r u". "
u". "Hi hello,how r u".

Encryption Time: 2.67
root@lokesh-Compaq-Presario-C700-Notebook-PC:/#
```

```
C is connected...
ivate Key: Fhk0EJ8+1dCsh2NBKJHy0jB/cwqxNCrBe8v9EjS4Piy
vE568CQQDk6EwTF7fwkQs6epKWFBRIYJoR3hksZhmDi9s0UksTPrv0cPtHNRSM
zPlb8lGapF5qDUakXNGNbd/FT+iC0nAkAjbjmvxjdeyzyL7HU3v8V7aBZ32WTn
qhZPMhSpYxnRL5u33dKWMsqJVtp7DkVVlbLgDpuJu8bzZNpUl39uiRAkAjN24q
sRUWQwYaBl3EWU+ytlNdx8/APs2nB+NAuMzpMR6f9GCCqLup0MPmwtF6QKwQUM
hG8CEOdZbsFPNBAkEAvIYc6XvUpZn0h44c45kk6P9k5fCIoBUSUXlYIis0+dcI
6R5UoWkQENr/nvYu7XJwcc8/boaiMy5NuFjzc93A==
---END RSA PRIVATE KEY-----

ne message received from Client 1
ter your id to retrieve half private key from SEM : manvi


equest is sent to SEM for half Private key...
lf private key received... decrypting message...
ceived Message : "Hi hello,how r u". "Hi hello,how r u". "Hi hello,ho
 hello,how r u".
cryption Time : 55.46
ot@lokesh-Compaq-Presario-C700-Notebook-PC:/#
```

Figure 6: Commands in other three terminals for 1024 bits on 2048 Modulus

V. PERFORMANCE ANALYSIS

IBE with mRSA is implemented with key sizes 512 bits, 1024 bits, 2048 bits on specific modulusand measured time to execute key generation, encrypt and decrypt operation. So, the IBE with mRSA takes very less time compared to other two schemes.

MODULUS	KEY SIZE	ENCRYPTION	DECRYPTION
512 Bits	512 Bits 1024 Bits 2048 Bits	1.89 2.63 5.64	13.94 54.92 253.47
1024 Bits	512 Bits 1024 Bits 2048 Bits	1.9 2.65 6.17	12.53 55.9 233.52
2048 Bits	512 Bits 1024 Bits 2048 Bits	1.91 2.67 5.55	14.25 55.46 266.78

Table 1 Comparison for 512, 1024, 2048 Bits on specific Modulus i.e 512.1024,2048

VI. CONCLUSIONS

Internet field is increasing day by day and the scope of cloud computing is also increasing in IT firms. Cloud computing provides the virtualization and on demand services to users. The only concern is to improve the security of the cloud by computing time for 512 bits, 1024 bits,2048 bits on specific modulus. Security issues related with the cloud environment are encryption, authentication of data and trust of vendor.

Key Generation operation uses Hash function to generate key, which increase time to generate key. So it's needed to find out encryption and decryption time for higher bits or alternative technique to find time. So that key generation time will be reduced and also encryption and decryption time.

ACKNOWLEDGEMENT

A project cannot be said to be work of an individual. A research is a combination of views and ideas, suggestions and contributions of many people. First of all, I would like to express my deep sense of respect and gratitude towards God and then to my guide, who has been the guiding force behind this work. I want to thank him for introducing me to the field of Computer Science and giving me the opportunity to work under him. I am greatly indebted to him for his constant encouragement and invaluable advice in every aspect of my academic life. His presence and optimism have provided an invaluable influence on my career and outlook for the future. I consider it my good fortune to have got an opportunity to work with such a wonderful person.

I would like to thank my classmates, from whom I learned a lot.

REFERENCES

[1] "Simple Identity-Based Cryptography with Mediated RSA", Xuhua Ding, Gene Tsudik (2003), CT-RSA LNCS 2612, Pages 192-209.

[2] Vidyanand Choudhary, "Software as a service: Implications for investment in software development In HICSS '07" Proceedings of the 40th Annual Hawaii International Conference on System Sciences, page 209a, Washington, DC, USA, 2007. IEEE Computer Society.

[3] "Identity-based Broadcast Encryption Scheme with Untrusted PKG", Shanqing Guo, Chunhua Zhang (2008), The 9th International Conference for Young Computer Scientists, Pages 1613-1618.

[4] V. Krishna Reddy, B. Thirumala Rao, Dr. L.S.S. Reddy and P. Sai Kiran , "Research Issues in Cloud Computing", *Global Journal of Computer Science and Technology, Vol. 11 No. 11* July 2011.

[5] A. Verma, L. Cherkasova, V. S. Kumar, and R. H. Campbell, "Performance-driven task co-scheduling for map reduce environments," in Network Operations and Management Symposium (NOMS), 2012 IEEE.

[6] Anitha Y, "Security Issues in Cloud Computing – A review", International Journal of Thesis projects and dissertations, Vol 1, Issue 1, Month October- December 2013.

[7] Elashry, I., Mu, Y. & Susilo, W. (2013). Identity-based mediated RSA revisited. Proceedings - 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (pp. 728-735). IEEE

[8] P. Subhasri, Dr. A. Padmapriya, "Implementation of Reverse Ceaser Cipher Algorithm for cloud computing", International Journal for advanced Research in Engineering and Technology, Vol-1, Issue VI, July-2013.

[9] K Hashizume et al., "An analysis of security issues for cloud computing", Journal of Internet Services and Applications, a Springer open journal, pp 1-13, 2013.

[10] Dr.A.Padmapriya, P.Subhasri," Cloud Computing: Reverse Caesar Cipher Algorithm to Increase Data Security", International Journal of Engineering Trends and Technology (IJETT) - Volume4, Issue4, pp 1067-1071, 2013.