IJCTA, 9(10), 2016, pp. 4545-4552
© International Science Press

Data Security for Cloud Using Public Key Cryptosystem

***Pachipala Yellamma **Dr Challa Narasimham ***Dr B.V .SubbaRao**

Abstract : Data storage paradigm in cloud computing brings many challenging issues on the security and storage. The critical nature of the cloud computing is to carries large amount of data through networks, the need is even more important. Security must be imposed on data by using encryption strategies to achieve secured data storage and access. In this paper we propose a system to securing data in cloud .In this method some important security services including key generation, encryption and decryption in cloud.

Keywords : Key generation, encryption, decryption, RSA, data security.

1. INTRODUCTION

Cloud computing is to increase capacity. Cloud computing is a service oriented architecture. Cloud computing is an on-demand information technology services and products. Data storage paradigm in cloud computing brings many challenging issues on the security and performance of the system. Securing data is always of plays an importance role. Data security is an important aspect of the quality of a service in cloud.

In our proposed system, we implement public key encryption algorithm, before storing the sensitive data in cloud. When the authorized user request the data for usage then data is decrypted and then provided to the end user.

1.1. Cryptography

Cryptography is the science of writing in secret code using mathematical theory and computer science practices by encompassing methods of transforming an intelligible message into an unintelligible message, and then retransforming that message back to its original form.

Three types of cryptographic schemes generally used to accomplish these goals:

1.2. Symmetric key Cryptography

In a secret key cryptosystems encryption and decryption use the same key. The principle who encrypts a message must share the encryption key(*ke*) with the principle who will be receiving and decrypting the encrypted message. The fact $ke \neq kd$.

1.3. Public key cryptography

Public key cryptosystem use two different keys, every key $ke\ \varepsilon$ K, There exists $kd\ \varepsilon\ K^1$, the two keys are different and match each other; the encryption key ke needn't be kept secret, and the principal who is the owner of ke can decrypt a cipher text encrypted under ke using the matching decryption key kd. The fact kd '" ke. The best known public-key cryptosystem is the RSA.

* Research scholar, Bharathiar University R&D Center, Coimbatore pachiapala.yamuna@gmail.com

** Professor, CSE, Dept Vegan's institute of science And Technology, vizag narasimham_c@yahoo.com

*** Professor IT Dept PVPSIT, Vijayawada. narasimham_c@yahoo.com

2. PROPOSED SYSTEM

In order to overcome the challenges in the existing cloud is security and less storage space. We have proposed new system for providing security and less storage space in cloud. In our work we providing security by using the public key algorithm RSA (Ron Rivest, Adi Shamir, Len Adleman).The RSA Algorithm provides the high security in high potential data encryption methodology.RSA is a public key cryptosystem that uses two keys namely public key and private key for Encryption and Decryption respectively. This ensures the high degree of security. Especially private key ensures the confidentiality, such that no other user (unauthorized) can view the uploaded file except the data owner.

Figure1 shows the proposed model, First the user has to first enter into the web page and request for registration. The user has to fill all the details and then submit the form then it will give the message registered successfully. If the user was already registered he can directly log in into the system and upload the file. User want to upload the file he/ she browse the file and click the upload button then it will display the message like file uploaded successfully and the cloud will generate the keys: public key & private key. The public key is published but the private key is sent to the user email which was given at the time of registration. That means the data is encrypted and the keys are generated. As soon as the user requests for the view files the cloud provider will ask for the private key. If the correct private key is given by the user, the cloud provider will decrypt the text file and displays it to the user. If the private key is wrong then it displays the encrypted data format only not the original file.

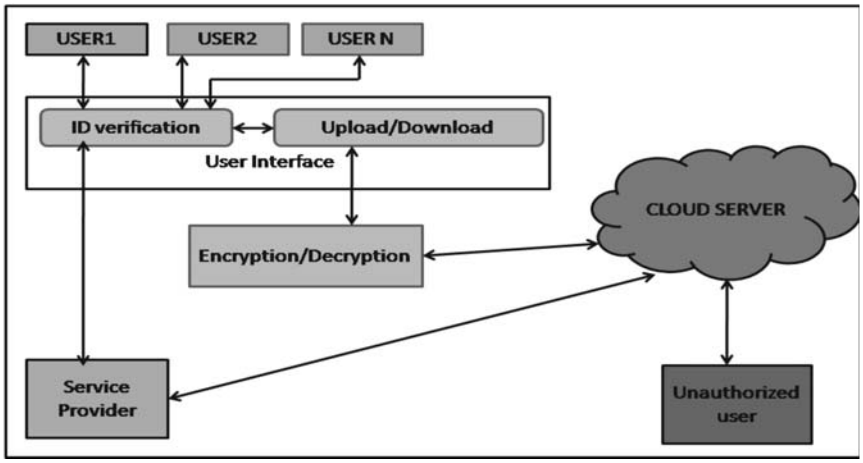
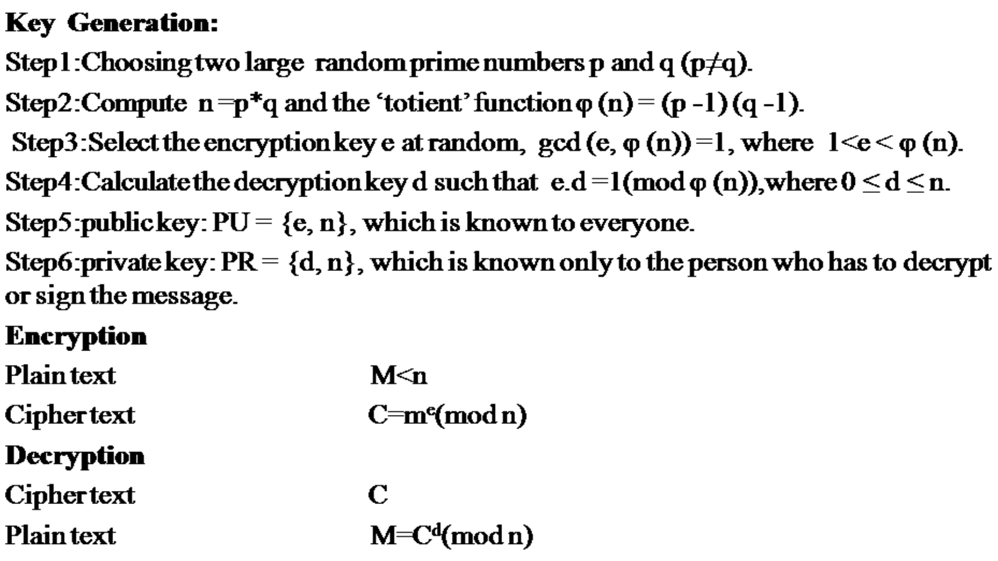


Fig. 1. Block diagram of proposed system.

2.1. Rsa Algorithm



Key Generation:

Step1:Choosing two large random prime numbers p and q ($p \neq q$).

Step2:Compute $n = p*q$ and the 'totient' function $\varphi(n) = (p-1)(q-1)$.

Step3:Select the encryption key e at random, $\gcd(e, \varphi(n)) = 1$, where $1 < e < \varphi(n)$.

Step4:Calculate the decryption key d such that $e.d = 1(\mathrm{mod}\ \varphi(n))$,where $0 \leq d \leq n$.

Step5:public key: $PU = \{e, n\}$, which is known to everyone.

Step6:private key: $PR = \{d, n\}$, which is known only to the person who has to decrypt or sign the message.

Encryption

Plain text	$M<n$
Cipher text	$C=m^e(\mathrm{mod}\ n)$

Decryption

Cipher text	C
Plain text	$M=C^d(\mathrm{mod}\ n)$

Fig. 2. The RSA Cryptosystem.

2.2. Detailed Design

A sequence diagram is an interaction diagram that shows how the processes are to be operate with one another and in what order. The construct of a message sequence chart is to represent the design in detailed. A sequence diagram shows object interactions is arranged in time sequence in an orderly manner.

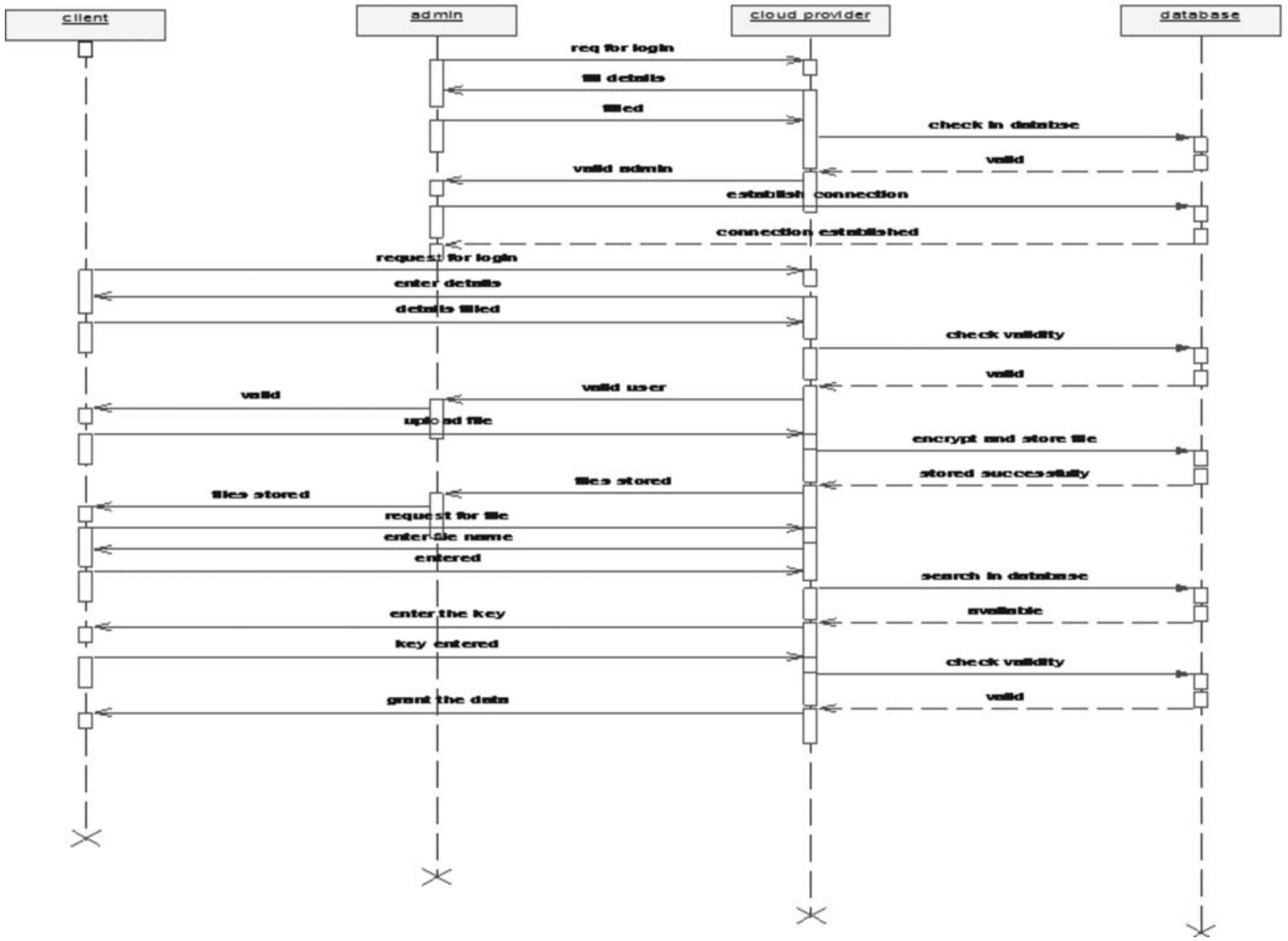


Fig. 3. Sequence diagram.

Initially the client will fill the login details. If he/she is authorized the users home page is displayed. The client will then upload file. By clicking browse the client will select the text file present in the system. After selecting the required file he/she will upload the file. The cloud will then encrypt the file and display a message file uploaded successfully. The public key is displayed itself and the private key is sent to the user's mail id.

2.3. RSA implementation

```
import java.math.BigInteger;
import java.security.SecureRandom;
public class RSA
{
private BigInteger n,d,e;
private int bitlen = 1024;
public RSA (BigInteger cn,BigInterger ce)
```

```
{
n = cn;
e = ce;
}
Public RSA (int bits)
{
bitlen = bits;
while (m.gcd(e).intValue()>1
{
public synchronized string encrypt (string message)
{
return string
}
public synchronized BigInteger encrypt(BigInteger message)
{
return message
}
public synchronized string decrypt (string message)
{
return new String
}
public synchronized BigInteger encrypt(BigInteger message)
{
return message
}
//Generate a new public and private key set
public synchronized void generatekeys()
{
while(m.gcd(e).intValues()>1
{
//calculate the  e and d value;
}
public static void main(String[] args)
{
RSA rsa = new RSA(1024);
}
```

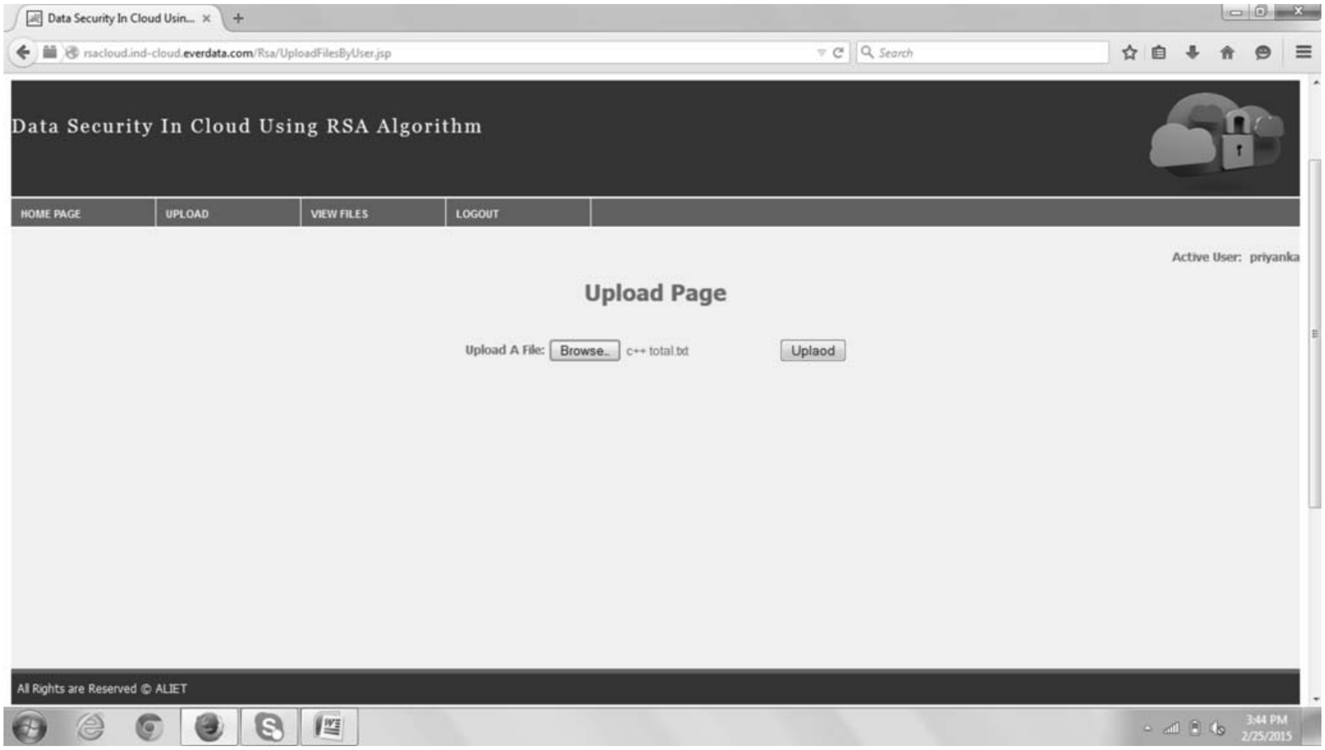
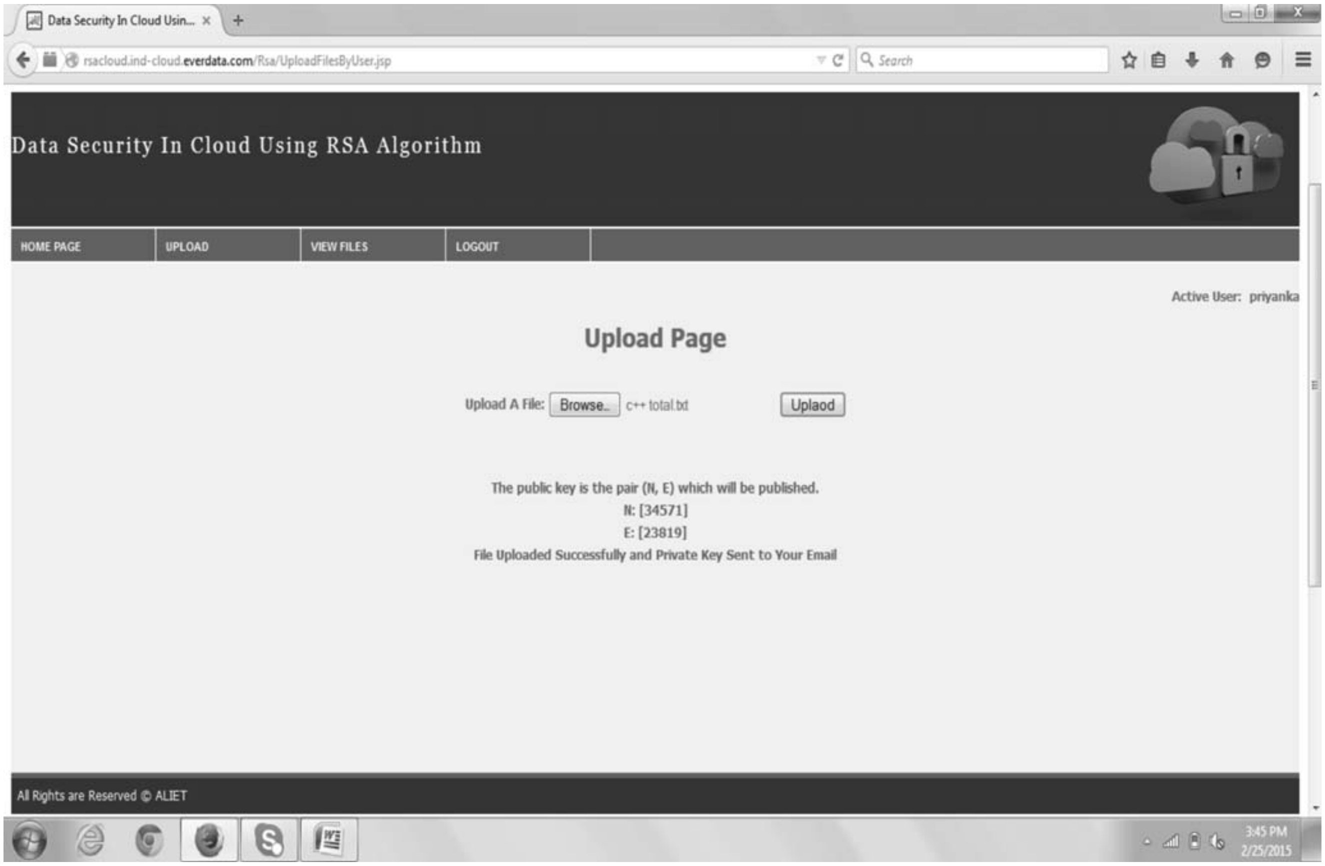
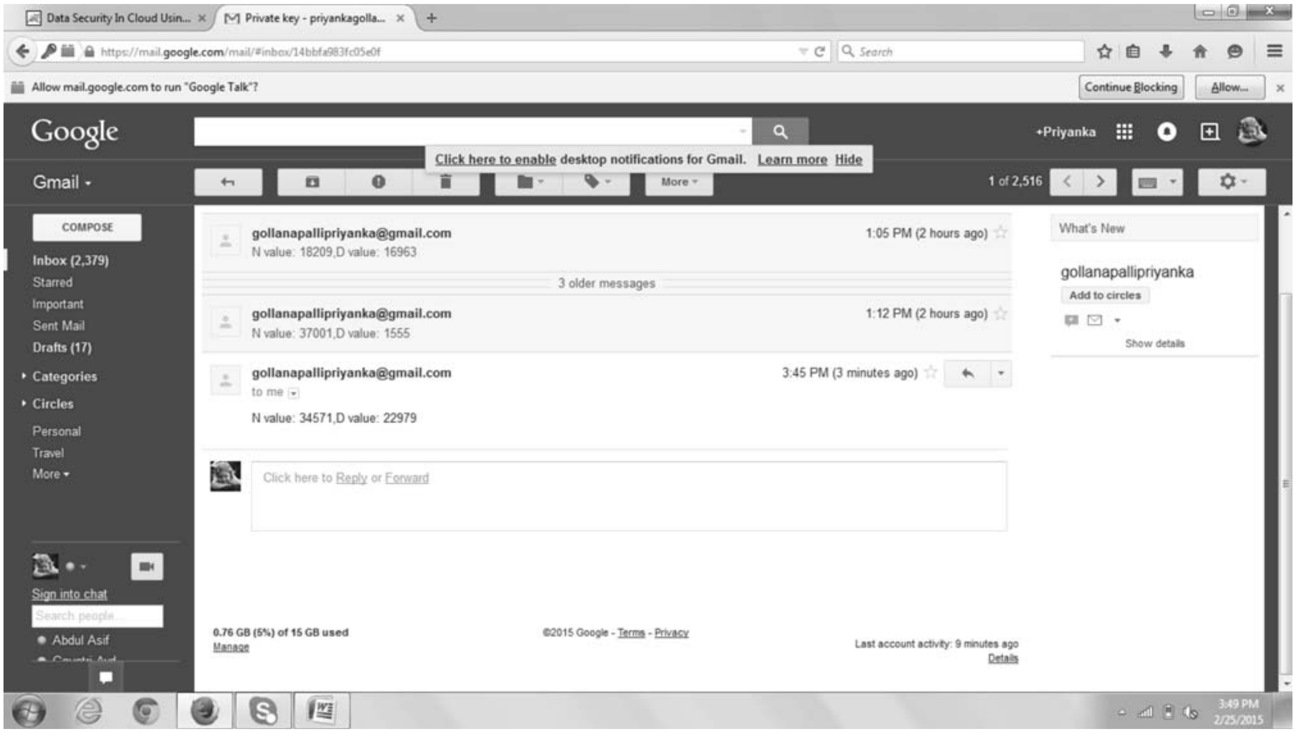

Data Security In Cloud Usin...
rsacloud.ind-cloud.everdata.com/Rsa/UploadFilesByUser.jsp
Search
Data Security In Cloud Using RSA Algorithm
HOME PAGE
UPLOAD
VIEW FILES
LOGOUT
Active User: priyanka
Upload Page
Upload A File:
Browse..
c++ total.txt
Uplaod
All Rights are Reserved © ALIET
3:44 PM
2/25/2015

Fig. 4. Upload the file.


Data Security In Cloud Usin...
rsacloud.ind-cloud.everdata.com/Rsa/UploadFilesByUser.jsp
Search
Data Security In Cloud Using RSA Algorithm
HOME PAGE
UPLOAD
VIEW FILES
LOGOUT
Active User: priyanka
Upload Page
Upload A File:
Browse..
c++ total.txt
Uplaod
All Rights are Reserved © ALIET
3:45 PM
2/25/2015

The public key is the pair (N, E) which will be published.
N: [34571]
E: [23819]
File Uploaded Successfully and Private Key Sent to Your Email

Fig. 5. File is encrypted and keys are generated.


Data Security In Cloud Usin...
Private key - priyankagolla...
https://mail.google.com/mail/#inbox/14bbfa983fc05e0f
Search
Allow mail.google.com to run "Google Talk"?
Continue Blocking
Allow...
Google
+Priyanka
Click here to enable desktop notifications for Gmail. Learn more Hide
Gmail
More
1 of 2,516
COMPOSE
Inbox (2,379)
Starred
Important
Sent Mail
Drafts (17)
Categories
Circles
Personal
Travel
More
Sign into chat
Search people...
Abdul Asif
What's New
gollanapallipriyanka
Add to circles
Show details
Click here to Reply or Forward
0.76 GB (5%) of 15 GB used
Manage
©2015 Google - Terms - Privacy
Last account activity: 9 minutes ago
Details
3:49 PM
2/25/2015

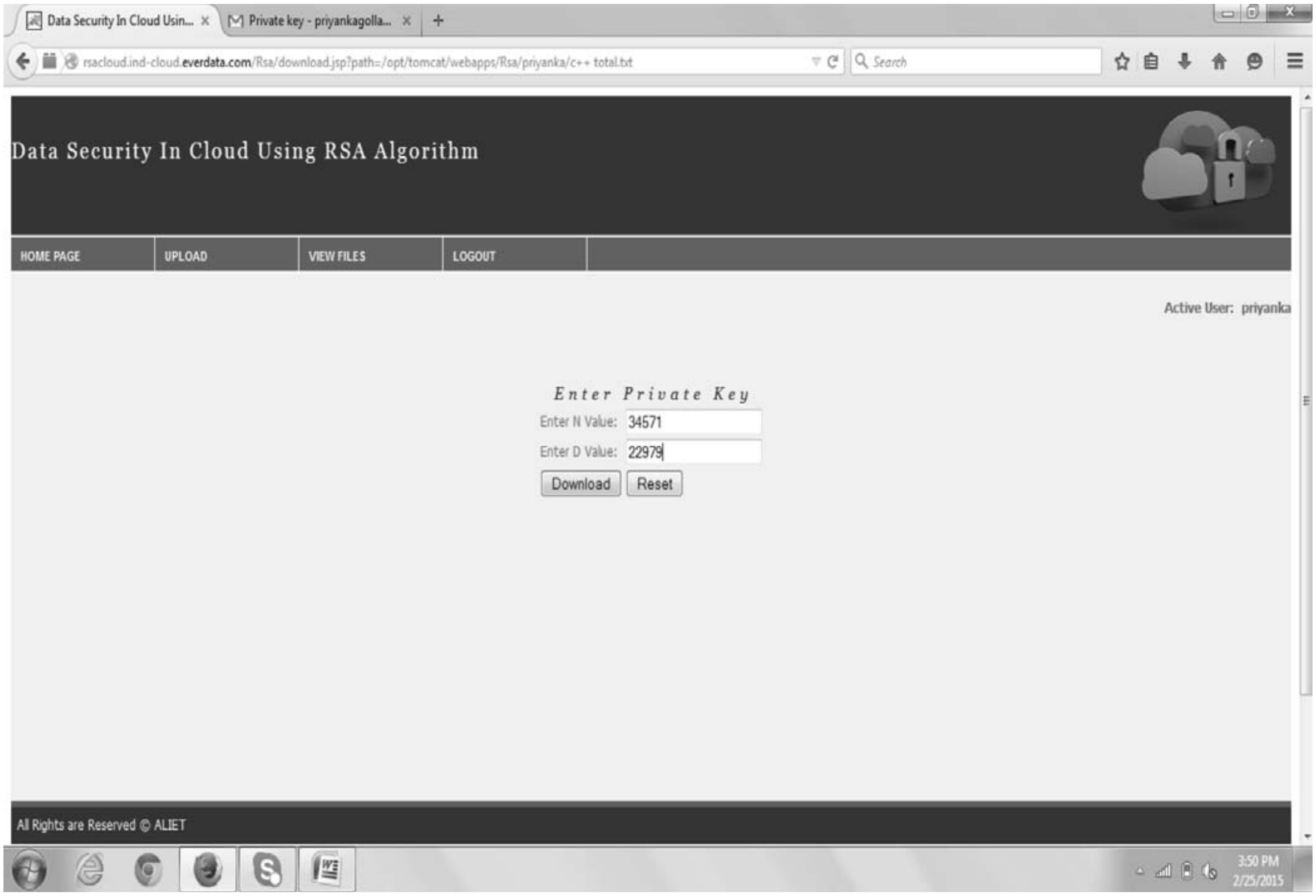
gollanapallipriyanka@gmail.com 1:05 PM (2 hours ago)
N value: 18209,D value: 16963

3 older messages

gollanapallipriyanka@gmail.com 1:12 PM (2 hours ago)
N value: 37001,D value: 1555

gollanapallipriyanka@gmail.com 3:45 PM (3 minutes ago)
to me
N value: 34571,D value: 22979

Fig. 6. Checking private key in the authorized user mail.


Data Security In Cloud Usin...
Private key - priyankagolla...
rsacloud.ind-cloud.everdata.com/Rsa/download.jsp?path=/opt/tomcat/webapps/Rsa/priyanka/c++ total.txt
Search
Data Security In Cloud Using RSA Algorithm
HOME PAGE
UPLOAD
VIEW FILES
LOGOUT
Download
Reset
All Rights are Reserved © ALIET
3:50 PM
2/25/2015

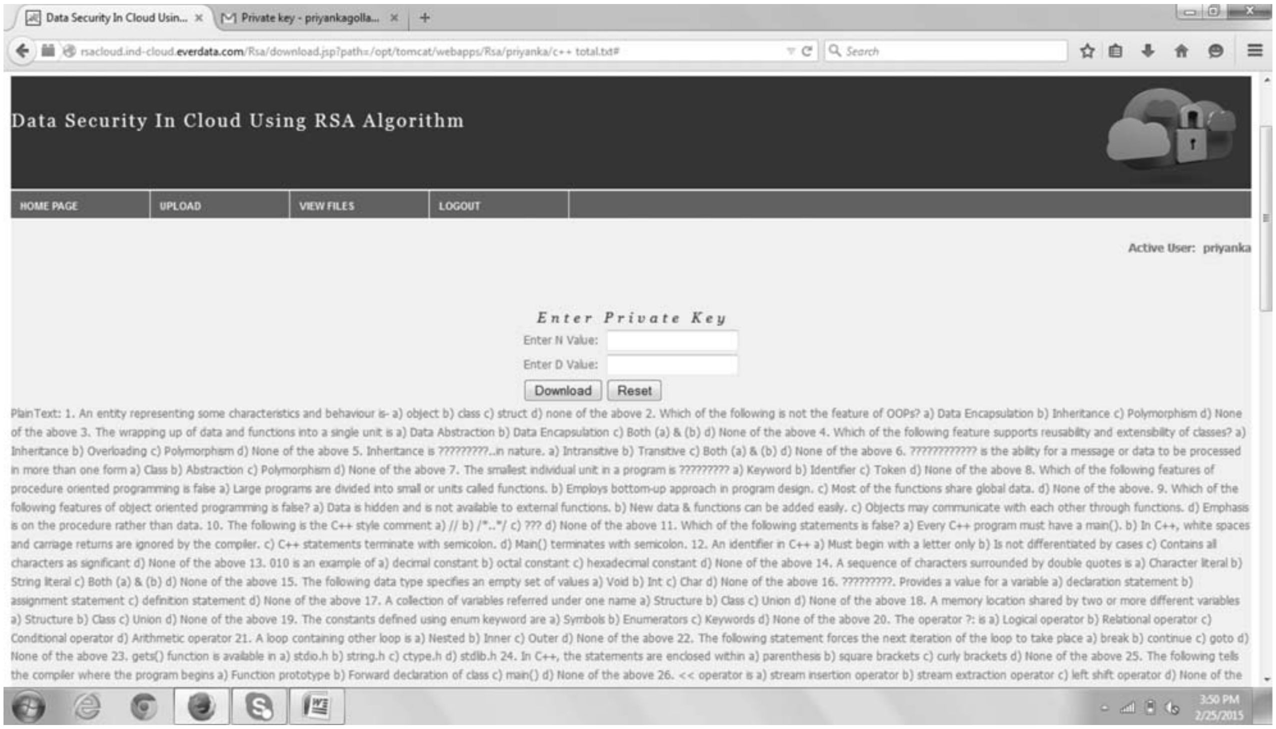
Active User: priyanka

Enter Private Key

Enter N Value: 34571

Enter D Value: 22979

Fig. 7. Entering valid private key.


Data Security In Cloud Usin...
Private key - priyankagolla...
rsacloud.ind-cloud.everdata.com/Rsa/download.jsp?path=/opt/tomcat/webapps/Rsa/priyanka/c++ total.txt#
Search
HOME PAGE
UPLOAD
VIEW FILES
LOGOUT
Download
Reset
3:50 PM
2/25/2015

Data Security In Cloud Using RSA Algorithm

Active User: priyanka

Enter Private Key

Enter N Value:

Enter D Value:

PlainText: 1. An entity representing some characteristics and behaviour is- a) object b) class c) struct d) none of the above 2. Which of the following is not the feature of OOPs? a) Data Encapsulation b) Inheritance c) Polymorphism d) None of the above 3. The wrapping up of data and functions into a single unit is a) Data Abstraction b) Data Encapsulation c) Both (a) & (b) d) None of the above 4. Which of the following feature supports reusabilty and extensibilty of classes? a) Inheritance b) Overloading c) Polymorphism d) None of the above 5. Inheritance is ?????????..in nature. a) Intransitive b) Transitive c) Both (a) & (b) d) None of the above 6. ???????????? is the abilty for a message or data to be processed in more than one form a) Class b) Abstraction c) Polymorphism d) None of the above 7. The smallest individual unit in a program is ????????? a) Keyword b) Identifier c) Token d) None of the above 8. Which of the following features of procedure oriented programming is false a) Large programs are divided into small or units called functions. b) Employs bottom-up approach in program design. c) Most of the functions share global data. d) None of the above. 9. Which of the following features of object oriented programming is false? a) Data is hidden and is not available to external functions. b) New data & functions can be added easily. c) Objects may communicate with each other through functions. d) Emphasis is on the procedure rather than data. 10. The following is the C++ style comment a) // b) /*..*/ c) ??? d) None of the above 11. Which of the following statements is false? a) Every C++ program must have a main(). b) In C++, white spaces and carriage returns are ignored by the compiler. c) C++ statements terminate with semicolon. d) Main() terminates with semicolon. 12. An identifier in C++ a) Must begin with a letter only b) Is not differentiated by cases c) Contains all characters as significant d) None of the above 13. 010 is an example of a) decimal constant b) octal constant c) hexadecimal constant d) None of the above 14. A sequence of characters surrounded by double quotes is a) Character literal b) String literal c) Both (a) & (b) d) None of the above 15. The following data type specifies an empty set of values a) Void b) Int c) Char d) None of the above 16. ?????????. Provides a value for a variable a) declaration statement b) assignment statement c) definition statement d) None of the above 17. A collection of variables referred under one name a) Structure b) Class c) Union d) None of the above 18. A memory location shared by two or more different variables a) Structure b) Class c) Union d) None of the above 19. The constants defined using enum keyword are a) Symbols b) Enumerators c) Keywords d) None of the above 20. The operator ?: is a) Logical operator b) Relational operator c) Conditional operator d) Arithmetic operator 21. A loop containing other loop is a) Nested b) Inner c) Outer d) None of the above 22. The following statement forces the next iteration of the loop to take place a) break b) continue c) goto d) None of the above 23. gets() function is available in a) stdio.h b) string.h c) ctype.h d) stdlib.h 24. In C++, the statements are enclosed within a) parenthesis b) square brackets c) curly brackets d) None of the above 25. The following tells the compiler where the program begins a) Function prototype b) Forward declaration of class c) main() d) None of the above 26. << operator is a) stream insertion operator b) stream extraction operator c) left shift operator d) None of the

Fig. 8. Retrieval of the data.

4. CONCLUSION

The RSA encryption algorithm is provides high data security and high control congestion between users and sever because a single server is used by multiple users. The private key is sent to the user mail account. Based on the private key and public key, the file is view and downloads from the cloud.

In future work, this technology allows for much more efficient computing by centralizing storage, memory, processing and bandwidth. My proposed algorithm is very help full to increase the performance in cloud computing.

5. REFERENCES

1. Dr.Challa Narasimham. ,Pachipala Yellamma., Data security in cloud using rsa 4th ICCCNT - 13July 4 - 6, 2013, Tiruchengode, India.
2. Esh Narayan,Mohit Malik,Aman Preet Singh,Prem Narain .,To enhance the data security of cloud in cloud computing using rsa algorithm. Bookman International Journal of Software Engineering, Vol. 1 No. 1 Sep. 2012 ISSN No. 2319-4278 © Bookman International Journals.
3. MuneshwaraM.S.,swethaM.S. , A Smarter Way of Securing and Managing Data for Cloud Storage Applications Using High Throughput Compression in the Cloud Environment., International Journal of Advance Research in Computer Science and Management Studies Volume 2, Issue 9, September 2014.
4. Dr. C.Narasimham, P.Yellamma., Performance Evaluation of Encryption Techniques and Uploading of Encrypted Data in Cloud. 4th ICCCNT - 13July 4 - 6, 2013, Tiruchengode, India.
5. The RSA Algorithm Evgeny Milanov3 June 2009.
6. S.monikandan,L.Arokiam.,Confidentiality technique to enhance security of data in public cloud storage using data obfuscation.,Indian journal of science and technology volume 8,issue 24,September 2015.
7. The RSA Solution for Cloud Security and Compliance AGRC foundation for VMware infrastructure security and compliance.
8. R.Kirubakaramoothi,D.Arivazhagan,D.Helen.,survey on encryption techniques used to secure cloud storage system.,Indian journal of science & Technology.,volume8,Issue 39,December 2015.
9. B. Hayes, Cloud computing, Comm. Acm, Vol. 51, No. 7,pp. 9–11, 2008.

10. IBM Software white paper (2013), Security intelligence is the smart way to keep the cloud safe.
11. Ramalingam sugumar,sharmila banu sheik Imam.,Symmetric Encryption Algoritham to Secure Outsourced Data in Public Cloud Storage. Indian Journal of Science &Technology volume8,Issue23,September 2015.
12. Tamizh M1, Elavarasi. K .,A Survey on Secure Authorized Deduplication for Outsourced Data in Hybrid Cloud., International Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 3, March 2015. ISSN (Online) 2278-1021ISSN (Print) 2319-5940.
13. Kuyoro S. O. Ibikunle F. Awodele O. Cloud Computing Security Issues and Challenges., International Journal of Computer Networks (IJCN), Volume (3) : Issue (5) : 2011.
14. Gurpreet Singh*1, Esh Narayan1, Aman Preet Singh., TO ENHANCE THE SECURITY IN CLOUD COMPUTING., International Journal of Engineering & Science Research., IJESR/July 2012/ Volume-2/Issue-7/Article No-13/626-633 ISSN 2277-2685.
15. MANDEEP KAUR#1, MANISH MAHAJAN#2., Using encryption Algorithms to enhance the Data Security in Cloud Computing., International Journal of Communication and Computer Technologies Volume 01 – No.12, Issue: 03 January 2013 ISSN NUMBER : 2278-9723
16. Nilesh N. Kumbhar ,Virendrasingh V. Chaudhari ,Mohit A.Badhe., The Comprehensive Approach for Data Security in Cloud Computing: A Survey., International Journal of Computer Applications (0975 – 8887) Volume 39– No.18, February 2012.
17. Mr. Abhishek Patial, Mr. Sunny Behal., RSA Algorithm achievement with Federal information processing Signature for Data protection in Cloud Computing., International Journal of Computers & Technology ISSN: 2277-3061 Volume 3. No. 1, AUG, 2012.
18. G. Jai Arul Jose1, C. Sajeev2, Dr. C. Suyambulingom3., Implementation of Data Security in Cloud Computing., International Journal of P2P Network Trends and Technology- Volume1Issue1- 2011