International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 06 Issue: 05 | May - 2022 Impact Factor: 7.185 ISSN: 2582-3930

Revocable IBE Scheme for Secure Data Sharing in Cloud Computing

Bhagyashri Babar [1]

Department of Computer Science and Engineering, N B Navale Sinhgad College of Engineering, Solapur,Maharashtra,India

ABSTRACT-Now days there are wide use of cloud computing for sharing the data. There are advantages of cloud computing technology. To directly outsource the shared data on cloud server there exist a natural resistance. Since the shared data contain valuable information. Thus, it is need to place cryptographically enhanced access control on the shared data. Identity-based encryption is a promising cryptographically primitive to build a practical data sharing system. However, access control is not static. That is, when some user's authorization is expired, there should be a mechanism that can remove him/her from the system. We analysis performance of proposed RSIBE scheme in terms of functionality and efficiency and will prove that it is feasible for practical and cost effective data sharing. At the end we demonstrate implementation result of proposed scheme.

Keywords cloud computing, cryptography, Identity-based encryption.

1.INTRODUCTION

Cloud computing provides large computation capacity and huge memory space at a usage per basis model. It enables users to get intended services anytime anywhere across multiple platforms, and thus brings great benefits to cloud users. Various service provider can offer a more flexible and share data over the Internet, which provides various benefits for our society . However, it also suffers from several security threats such as,

- Data sharing is often implemented in an open and hostile environment, and cloud server would become a target of attacks. Sometimes cloud server itself may reveal users' data for illegal profit.
- Data sharing is not static. That is, when a user's authorization gets expired, he/she should no longer possess the privilege of accessing the previously and subsequently shared data. Therefore, while outsourcing data to cloud server, users also want to control access to these data such that only those currently authorized users can share the outsourced data.

A solution to problem is we propose identity-based cryptographically System to achieve the security goals. In proposed system cryptographically enforced access control such as identity-based encryption (IBE). Furthermore, to over come the security threats, such kind of identity-based access control placed on the shared data should meet the Data confidentiality, Backward secrecy, Forward secrecy .

Example. Data provider i.e. Team Leader can share documents with team member working on project and can collaborate with each other effectively

The architecture of Data sharing is represented in below fig 1.1

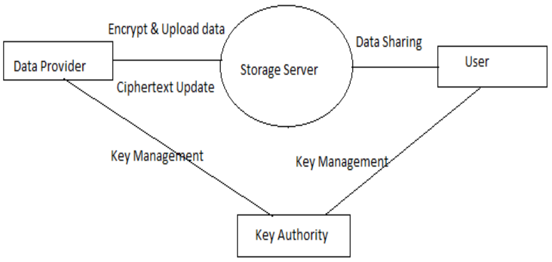


Fig 1.1

2.METHODOLOGY

In this proposed system we are using Cryptography method which means protecting information and communications through the use of codes, so that only those for whom the information is intended can read and process it. cryptography in other words, secure information and communication techniques derived from mathematical concepts and a set of rule-based calculations called algorithms, to transform messages in ways that are hard to decipher. These deterministic algorithms are used for cryptographic key generation, digital signing, verification to protect data privacy, web browsing on the internet and confidential communications such as credit card transactions and email.

Cryptographic algorithms

Cryptosystems use a set of procedures known as cryptographic algorithms, to encrypt and decrypt messages to secure communications among computer systems, devices and applications. A cipher suite uses following algorithm for encryption, message authentication and key exchange

- public and private key generation for data encryption/decryption

- digital signing and verification for message authentication
- key exchange

Cryptography Techniques

Cryptography is closely related to the disciplines of cryptology and cryptanalysis. It includes techniques such as microdots, merging words with images and other ways to hide information in storage or transit. However, in today's computer-centric world, cryptography is most often associated with scrambling plaintext into cipher text. Modern cryptography concerns itself with the following four objectives, **Confidentiality, Integrity, Non-repudiation, Authentication.**

1. Single-key or symmetric-key encryption algorithms- Both the sender and receiver share a single key. The sender uses this key to encrypt plaintext and send the cipher text to the receiver. On the other side the receiver applies the same key to decrypt the message and recover the plain text. Example . Advanced Encryption Standard (AES).

2. Public-key or asymmetric-key encryption algorithms- It's uses a pair of keys, a public key associated with the creator/sender for encrypting messages and a private key that only the originator knows (unless it is exposed or they decide to share it) for decrypting that information. Examples RSA, used widely on the internet, Digital Signature Algorithm ,Diffie-Hellman key exchange.

3.MODELING AND ANALYSIS

CRYPTOGRAPHY HASH FUNCTION

Hash functions are extremely useful and appear in almost all information security applications. A hash function is a mathematical function that converts a numerical input value into another compressed numerical value. The input to the hash function is of arbitrary length but output is always of fixed length. Values returned by a hash function are called **message digest** or simply **hash values .**

Example of cryptography hash function includes authenticating digital signatures to gain access to digital documents, verifying message and file integrity, and storing and verifying passwords, etc. Digital signatures work on the premise that the sender, after satisfying the necessary prerequisites of authentication, provides the receiver with the required data without getting it altered in the process. The same process takes place for password and file verification using input values compared to their corresponding specific hash values.

KUnodes Algorithm

In the proposed system, used a mechanism revocable-storage identity-based encryption (RSIBE) and KUNode algorithm for building a cost-effective data sharing system .It enables a data provider to add the current time period to the cipher text such that the receiver can decrypt the cipher text within that time period. and its corresponding security model; and backward/forward secrecy simultaneously. :

We can provide formal definitions for RSIBE KUNODES ALGORITHM: By using this algorithm only non-revoked user at a time period are able to decrypt the cipher text.

INPUT: Binary tree revocation list, Time period

OUTPUT: outputs the smallest subset Y of nodes of BT such that Y contains an ancestor for each node that is not revoked before the time period t.

STEP 1: Data provider upload the file in cloud with validity time

2. Data user access the data.

2.1. if the user tries to access the data within a specified time only he/she is able to access the data

2.2. Otherwise data provider need to update the key.

3. Data provider update the key used by the user.

4. Then he will update the cipher text. This will provide both forward and backward security to the data stored in a cloud.

By this algorithm ,when we revoke the leaf node their ancestors also get updated and the node which shares the same key of revoked node also get updated.

Algorithm 1 KUNodes(BT, RL, t)

```
$X,Y \leftarrow - \emptyset$
for all $(\eta i ,ti) \in RL$ do
  if $ti \leq t$ then
    Add Path($\eta i$) to X
  end if
end for
for all $\theta \in X$ do
  if $\theta l \in / X$ then
    Add $\theta l$ to Y
  end if
```

```
11. : if θr∈/X then
12. : Add θr to Y
13. : end if
14. : end for
15. : if Y=∅ then
16. : Add the root node ε to Y
17. : end if
18. : return Y
```

DEFINITION IN RS-IBE

A Revocable IBE Scheme for Secure Data Sharing in Cloud Computing with message space M, identity space I and total number of time periods T is comprised of the following seven polynomial time algorithms

[1]Setup(1λ , T, N): the setup algorithm takes as input the security parameter λ ,the time bound T and the maximum number of system users N , and it outputs the public parameter P P and the master secret key MSK, associated with the initial revocation list RL=∅ and state st.

[2] PKGen(P P, M SK, ID): The private key generation algorithm takes as input P P , M SK and an identity ID∈I, and it generates a private key SKID for ID and an updated state st.

[3] KeyUpdate(P P, M SK, RL, t, st): The key update algorithm takes as input P P , M SK, the current revocation list RL, the key update time t≤T and the state st, it outputs the key update KUt

[4]DKGen(P P, SKID, KUt): The decryption key generation algorithm takes as input P P , SKID and KUt ,and it generates a decryption key DKID,t for ID with time period t or a symbol ⊥ to illustrate that ID has been previously revoked.

[5]Encrypt(P P, ID, t, M): The encryption algorithm takes as input P P , an identity ID, a time period t≤T , and a message M∈M to be encrypted, and outputs a cipher text CTID,t.

[6] CTUpdate(P P, CTID,t, t′): The cipher text update algorithm takes as input P P , CTID,t and a new time period t ′ ≥ t, and it outputs an updated cipher textCTID,t′ .

[7]Decrypt(P P, CTID,t, DKID,t′): The decryption algorithm takes as input P P , CTID,t, DKID,t′ , and it recovers the encrypted message M or a distinguished symbol ⊥ indicating that CTID,t is an invalid cipher text.

[8]Revoke(P P, ID, RL, t, st): The revocation algorithm takes as input P P , an identity ID∈I to be revoked, the current revocation list RL, a state st and revocation time period t≤T , and it updates RL to a new one

4. EXPERIMENTS EXECUTION & RESULTS

Sec I

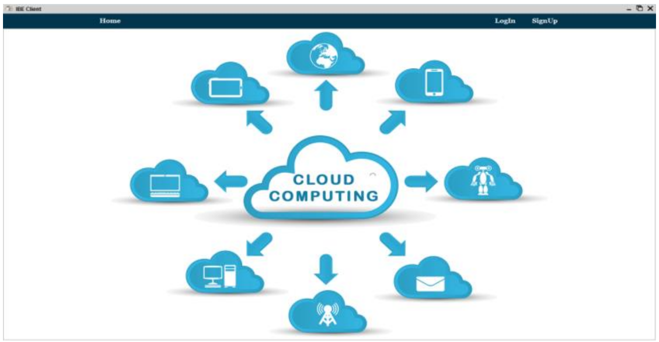
System Users

1. Data provider

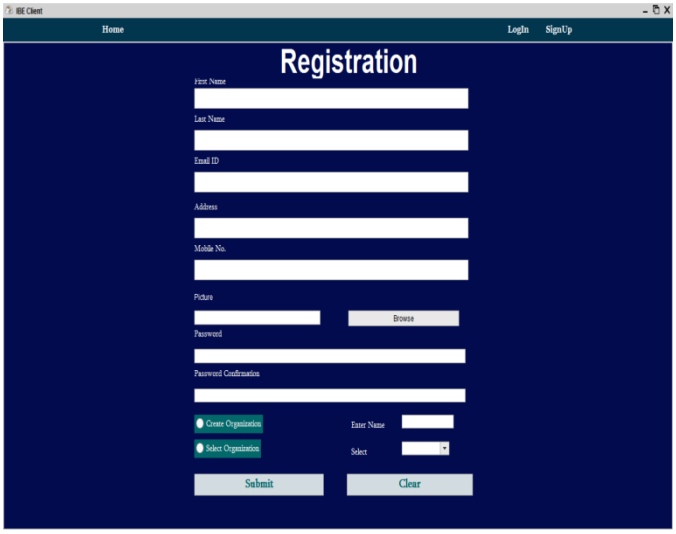
2. User

3. Key Distributer login

1. Login Window



2. Sign Up



Registration

First Name

Last Name

Email ID

Address

Mobile No.

Picture

Browse

Password

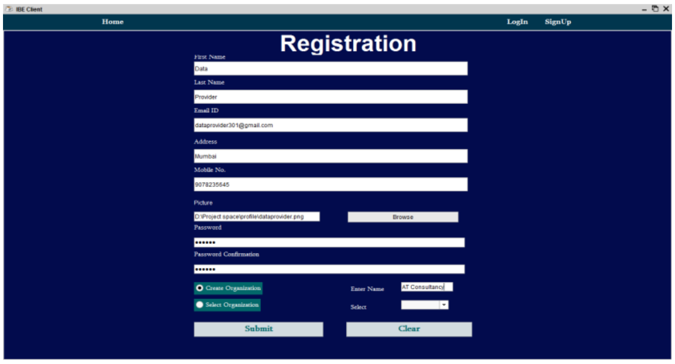
Password Confirmation

○ Create Organization Enter Name

○ Select Organization Select

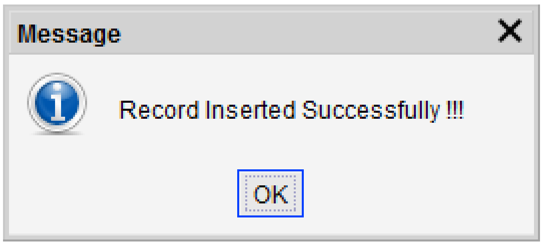
Submit Clear

2.1 Create **AT Consultancy**



Registration

First Name
Data
Last Name
Provider
Email ID
dataprovider301@gmail.com
Address
Mumbai
Mobile No.
9078235645
Picture
D:\Project space\profile\dataprovider.png
Password
••••••
Password Confirmation
••••••
● Create Organization
○ Select Organization
Enter Name AT Consultancy
Select



Message

Record Inserted Successfully !!!

2.1.1. Add 4 user in AT Consultancy

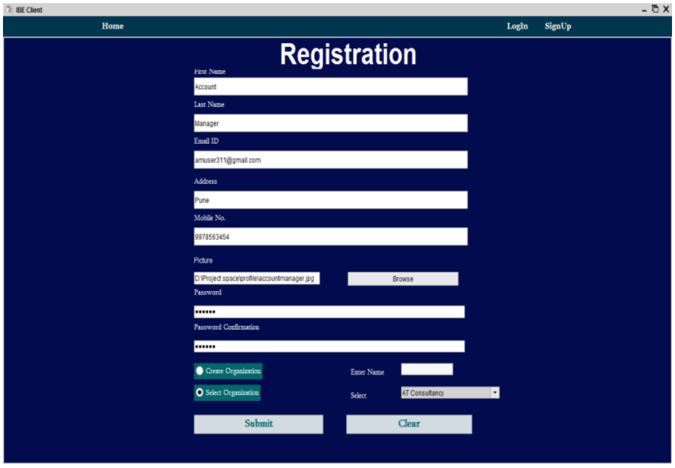
i)Account Manager

ii)Compliance Manager

iii)Account Assistant

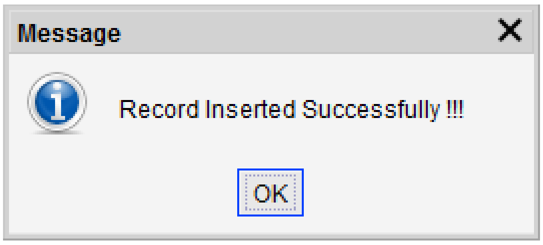
iv)Compliance Assistant

i)Account Manager



Registration

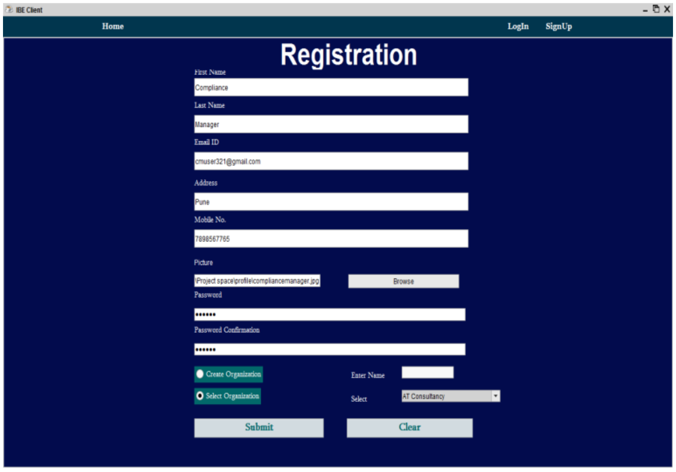
First Name
Account
Last Name
Manager
Email ID
amuser311@gmail.com
Address
Pune
Mobile No.
9978563454
Picture
D:\Project space\profile\accountmanager.jpg
Password
••••••
Password Confirmation
••••••
○ Create Organization
● Select Organization
Enter Name
Select AT Consultancy



Message

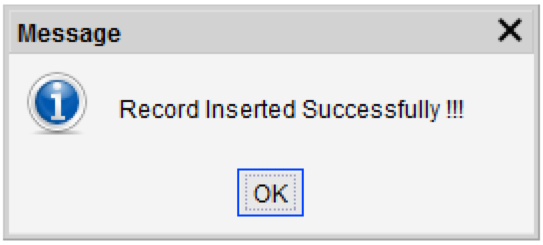
Record Inserted Successfully !!!

ii)Compliance Manager



Registration

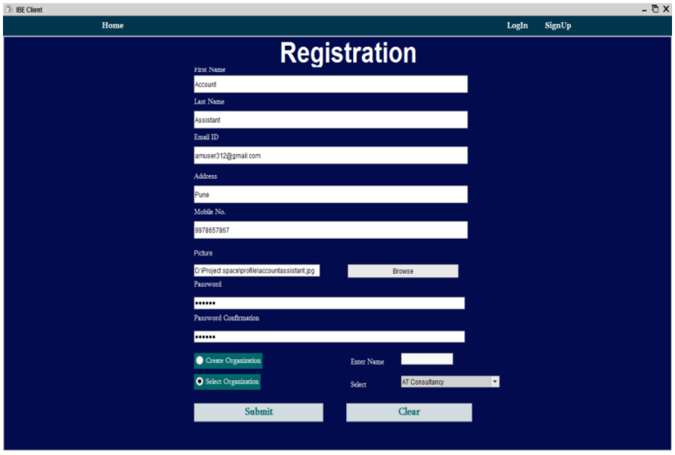
First Name
Compliance
Last Name
Manager
Email ID
cmuser321@gmail.com
Address
Pune
Mobile No.
7898567765
Picture
\Project space\profile\compliancemanager.jpg
Password
••••••
Password Confirmation
••••••
○ Create Organization
● Select Organization
Enter Name
Select AT Consultancy



Message

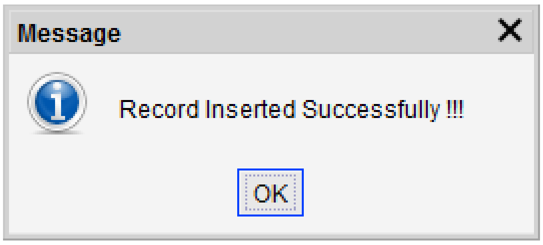
Record Inserted Successfully !!!

iii)Account Assistant



Registration

First Name
Account
Last Name
Assistant
Email ID
amuser312@gmail.com
Address
Pune
Mobile No.
9978657867
Picture
D:\Project space\profile\accountassistant.jpg
Password
••••••
Password Confirmation
••••••
○ Create Organization
● Select Organization
Enter Name
Select AT Consultancy

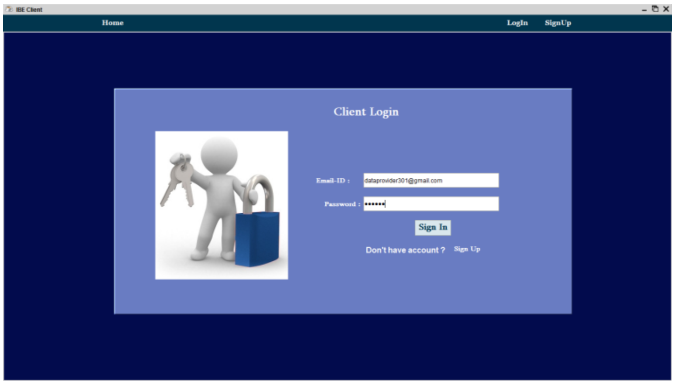


Message

Record Inserted Successfully !!!

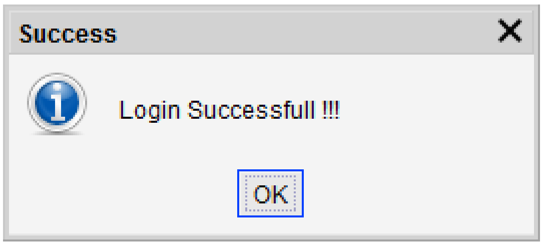
iv) Similarly for Compliance Assistant

3. now we login as **AT consultancy(Data Provider)** which is organization ,going to share file with user **Account Manager** only .



Email-ID : dataprovider301@gmail.com

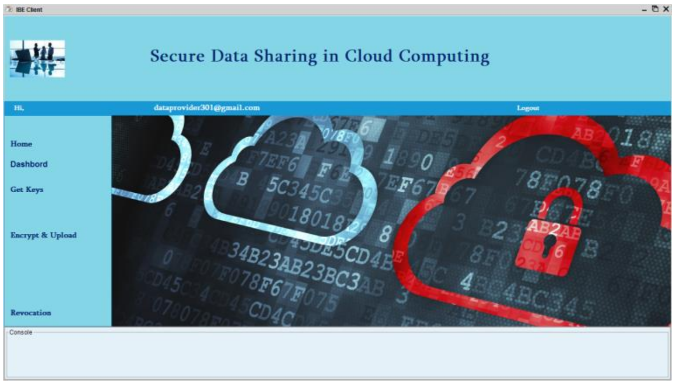
Password : ••••••



Success

Login Successfull !!!

4.after successfully login : Home tab will appear like this

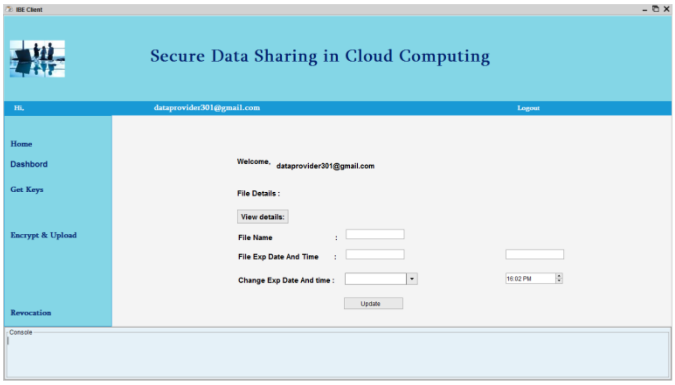


Secure Data Sharing in Cloud Computing

Hi, dataprovider301@gmail.com

5.Dashboard tab

Shared files details will be appear here



Secure Data Sharing in Cloud Computing

Hi, dataprovider301@gmail.com

Welcome, dataprovider301@gmail.com

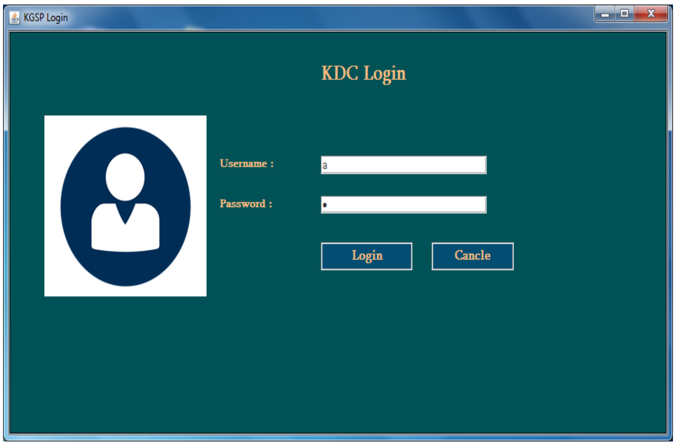
File Details :

File Name :

File Exp Date And Time :

Change Exp Date And time : 16:02 PM

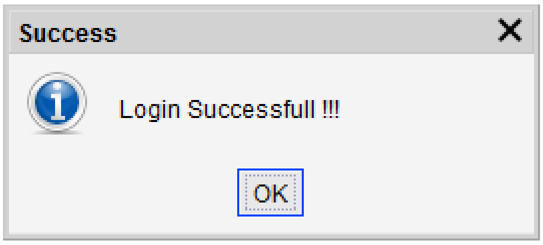
6.key distributer login



KDC Login

Username : a

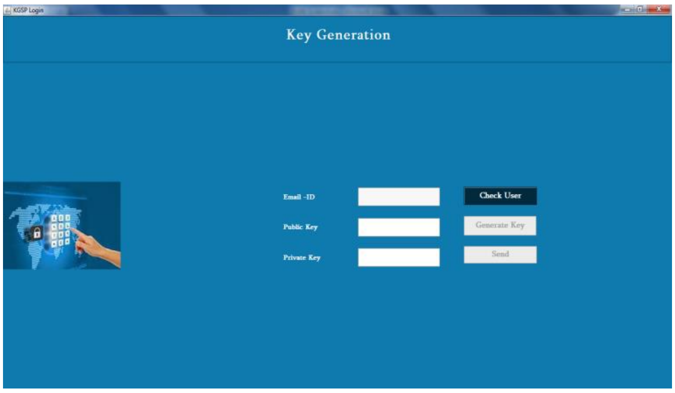
Password : •



Success

Login Successfull !!!

After Successfully Login Key distributer window will appear like this



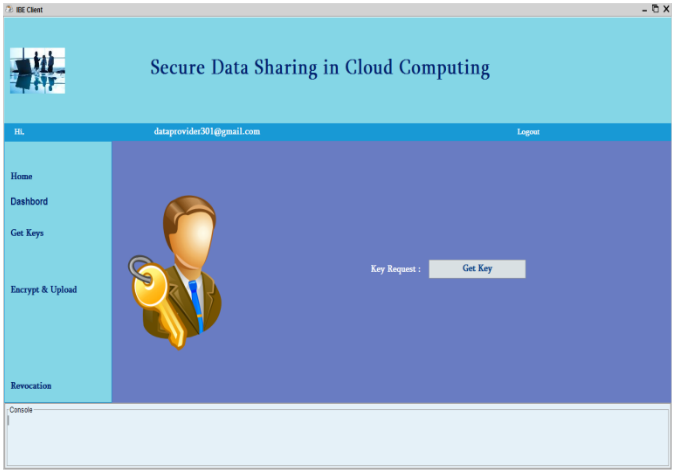
Key Generation

Email -ID

Public Key

Private Key

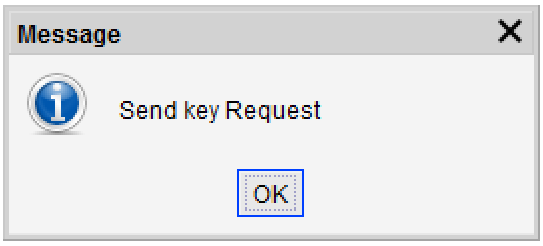
7. If AT consultancy want to share file to with only Account Manager then first he will get key for Account Manager



dataprovider301@gmail.com

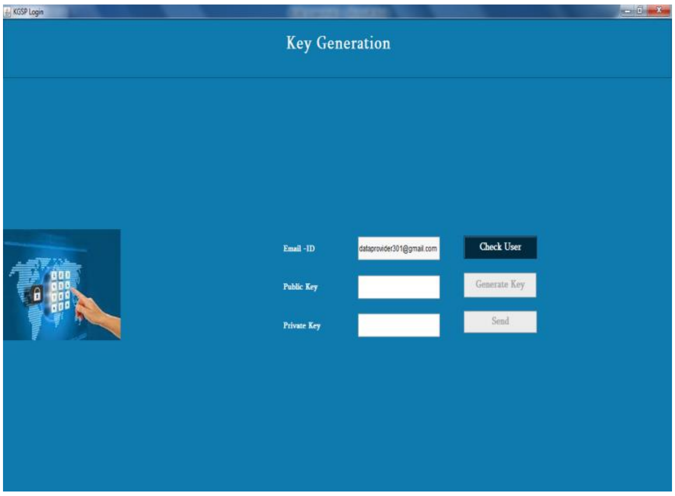
Key Request :

Data Provider will Click Get Key Button then Request for key will send to Key distributer



Message

Send key Request

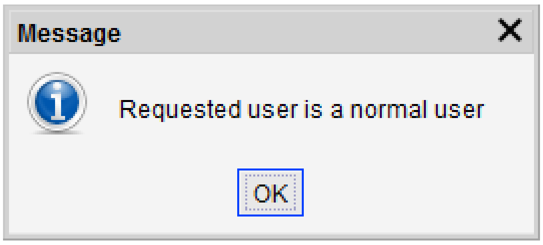


Email -ID: dataprovider301@gmail.com

Public Key:

Private Key:

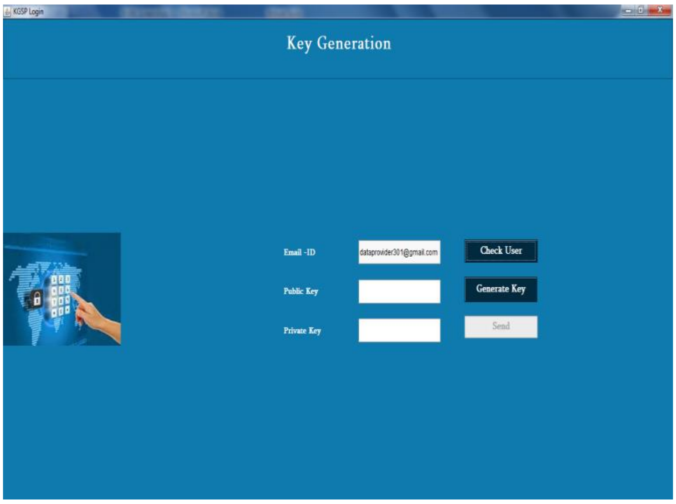
After click on **check user** button



Message

Requested user is a normal user

And **Generate key** button is visible

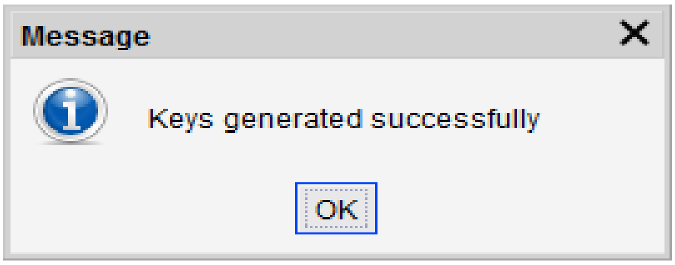


Email -ID: dataprovider301@gmail.com

Public Key:

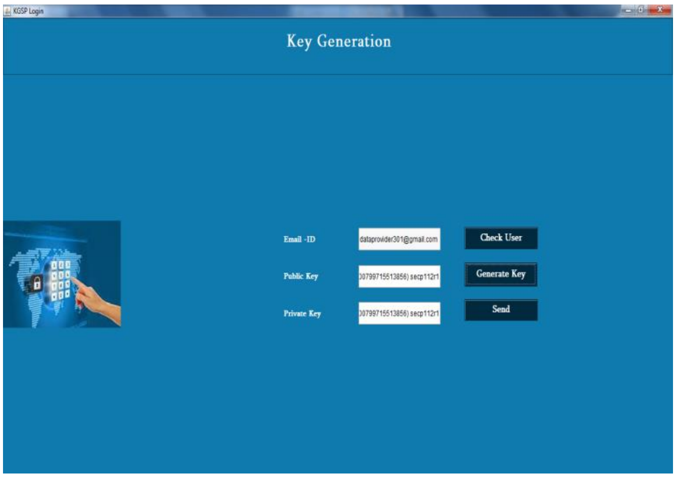
Private Key:

After clicking **Generate key** button



Message

Keys generated successfully

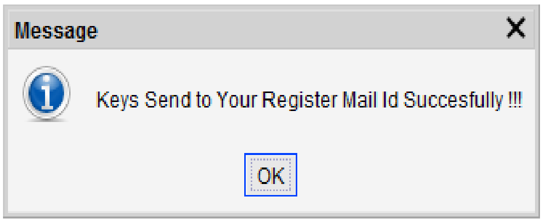


Email -ID: dataprovider301@gmail.com

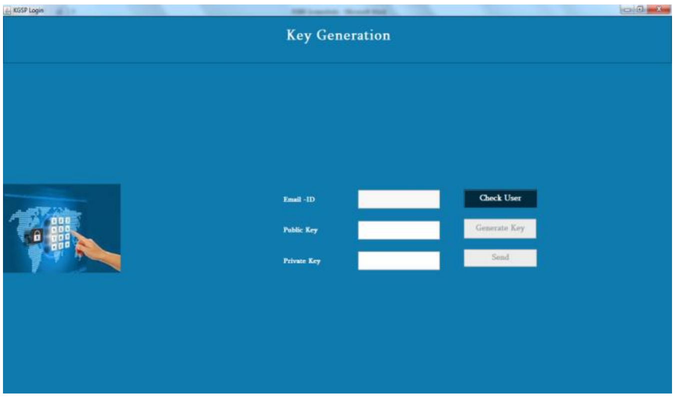
Public Key:)0799715513856) secp112r1

Private Key:)0799715513856) secp112r1

After clicking on send button

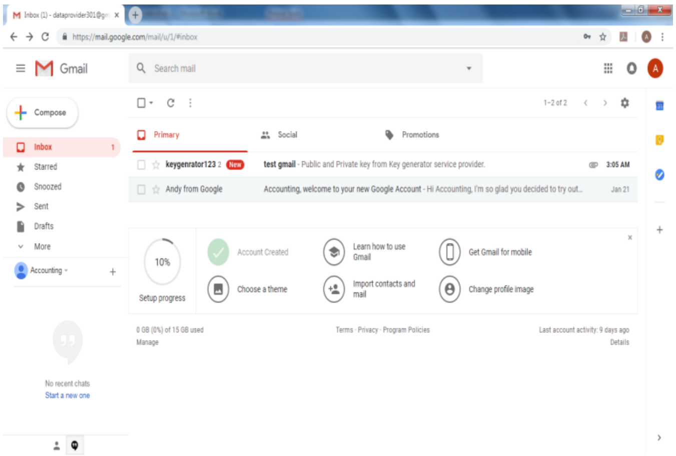

Message

Keys Send to Your Register Mail Id Succesfully !!!


Key Generation

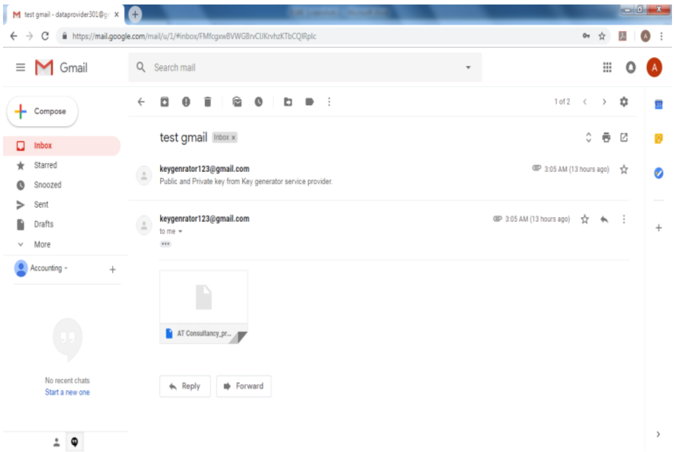
After Sending Key to register Email id window will appear like this

8. Key send Gmail account key gen send key


https://mail.google.com/mail/u/1/#inbox

keygenrator123 2 New — test gmail - Public and Private key from Key generator service provider. — 3:05 AM

Andy from Google — Accounting, welcome to your new Google Account - Hi Accounting, I'm so glad you decided to try out... — Jan 21


https://mail.google.com/mail/u/1/#inbox/FMfcgxwBVWGBrvCIJKrvhzKTbCQIRplc

test gmail Inbox

keygenrator123@gmail.com — 3:05 AM (13 hours ago)
Public and Private key from Key generator service provider.

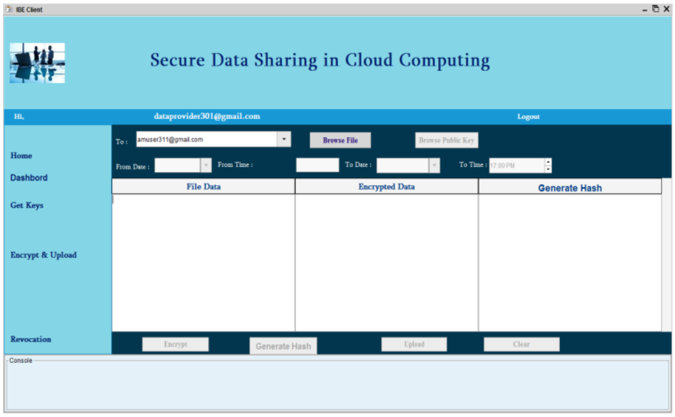
keygenrator123@gmail.com — 3:05 AM (13 hours ago)
to me

AT Consultancy_pr...

Data Provider will download public and private key.

Using this key data provider will encrypt input file.

9. Encrypt and upload

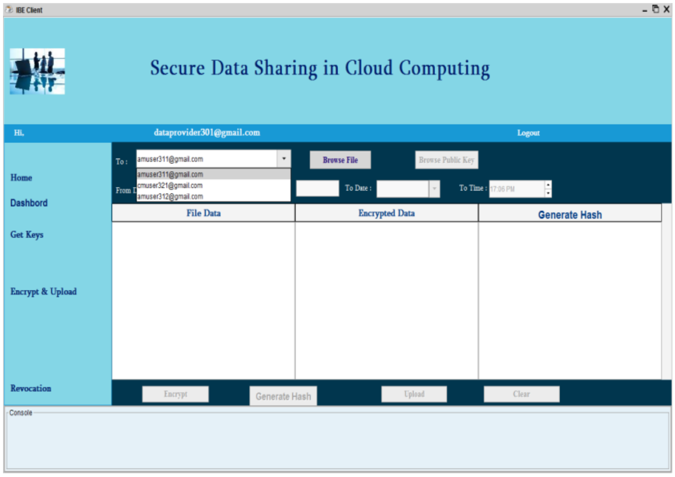

Secure Data Sharing in Cloud Computing

Hi, dataprovider301@gmail.com

To : amuser311@gmail.com

To Time : 17:00 PM

- Select user as amuser311@gmail.com


Secure Data Sharing in Cloud Computing

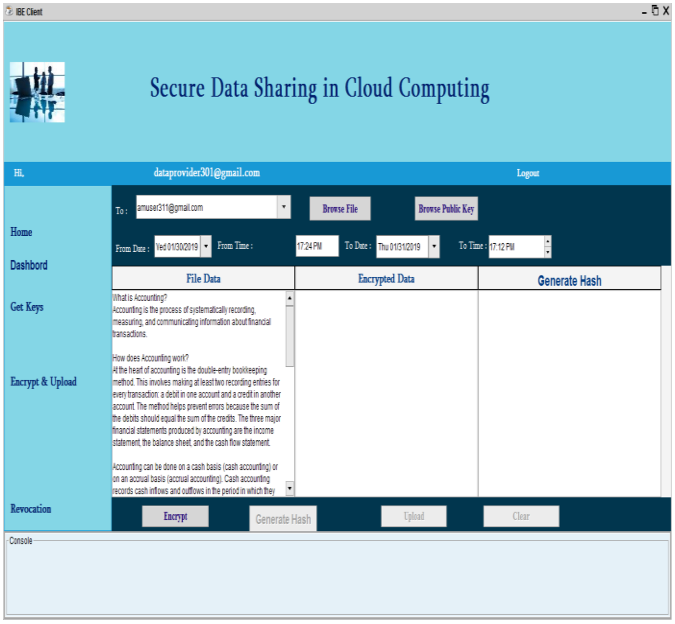
Hi, dataprovider301@gmail.com

To : amuser311@gmail.com

amuser311@gmail.com
amuser321@gmail.com
amuser312@gmail.com

To Time : 17:06 PM

- Browse File to be share and set timestamp



Hi, dataprovider301@gmail.com

To : amuser311@gmail.com

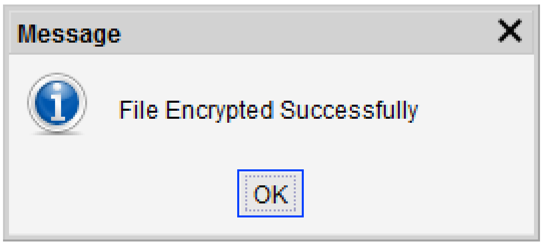
From Date : Ved 01/30/2019 From Time : 17:24 PM To Date : Thu 01/31/2019 To Time : 17:12 PM

What is Accounting?
Accounting is the process of systematically recording, measuring, and communicating information about financial transactions.

How does Accounting work?
At the heart of accounting is the double-entry bookkeeping method. This involves making at least two recording entries for every transaction: a debit in one account and a credit in another account. The method helps prevent errors because the sum of the debits should equal the sum of the credits. The three major financial statements produced by accounting are the income statement, the balance sheet, and the cash flow statement.

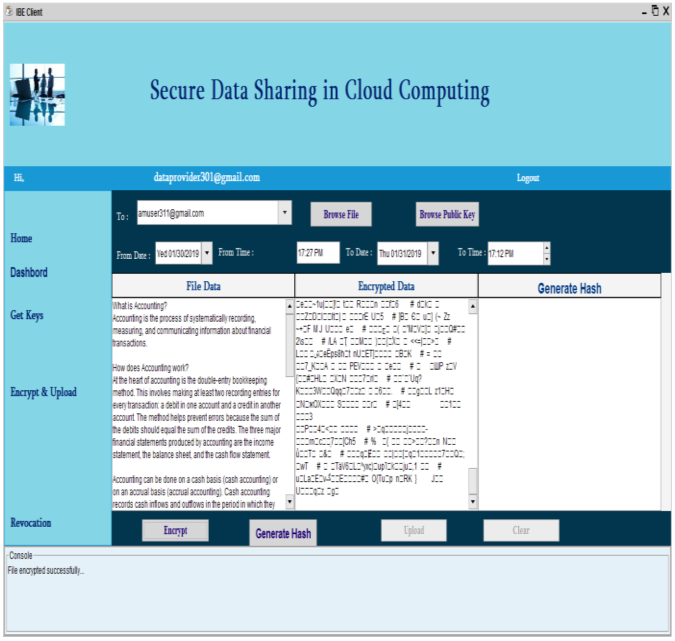
Accounting can be done on a cash basis (cash accounting) or on an accrual basis (accrual accounting). Cash accounting records cash inflows and outflows in the period in which they

Click Encrypt Button



File Encrypted Successfully

- **Generate Hash** button will visible



Hi, dataprovider301@gmail.com

To : amuser311@gmail.com

From Date : Ved 01/30/2019 From Time : 17:27 PM To Date : Thu 01/31/2019 To Time : 17:12 PM

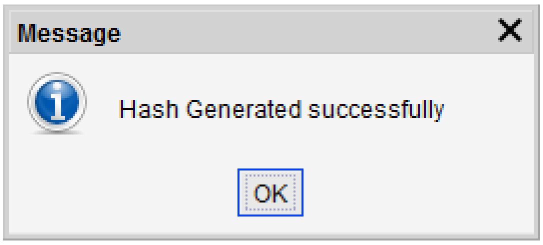
What is Accounting?
Accounting is the process of systematically recording, measuring, and communicating information about financial transactions.

How does Accounting work?
At the heart of accounting is the double-entry bookkeeping method. This involves making at least two recording entries for every transaction: a debit in one account and a credit in another account. The method helps prevent errors because the sum of the debits should equal the sum of the credits. The three major financial statements produced by accounting are the income statement, the balance sheet, and the cash flow statement.

Accounting can be done on a cash basis (cash accounting) or on an accrual basis (accrual accounting). Cash accounting records cash inflows and outflows in the period in which they

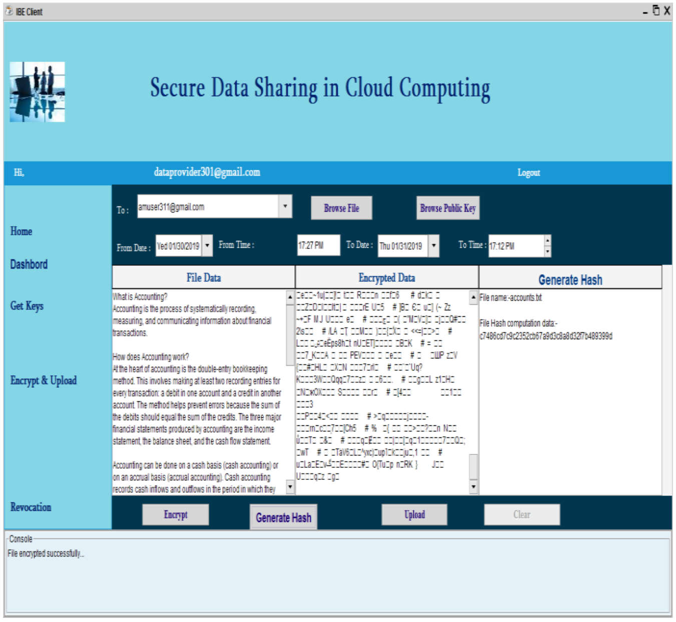
File encrypted successfully..

Click Generate Hash button



Hash Generated successfully

- Upload button will visible



Hi, dataprovider301@gmail.com

To : amuser311@gmail.com

From Date : Ved 01/30/2019 From Time : 17:27 PM To Date : Thu 01/31/2019 To Time : 17:12 PM

What is Accounting?
Accounting is the process of systematically recording, measuring, and communicating information about financial transactions.

How does Accounting work?
At the heart of accounting is the double-entry bookkeeping method. This involves making at least two recording entries for every transaction: a debit in one account and a credit in another account. The method helps prevent errors because the sum of the debits should equal the sum of the credits. The three major financial statements produced by accounting are the income statement, the balance sheet, and the cash flow statement.

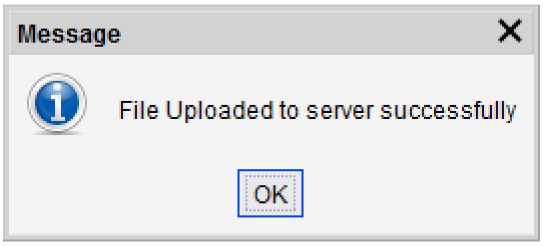
Accounting can be done on a cash basis (cash accounting) or on an accrual basis (accrual accounting). Cash accounting records cash inflows and outflows in the period in which they

File name:-accounts.txt

File Hash computation data:-
c7486cd7c9c2352cb67a9d3c8a8d32f7b489399d

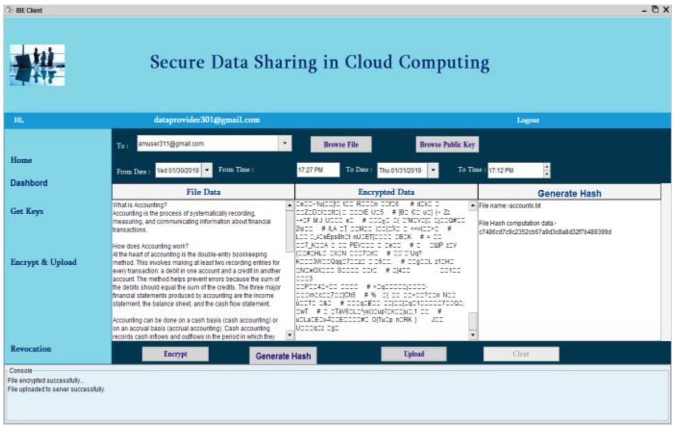
File encrypted successfully..

Click upload button



File Uploaded to server successfully

- It will display acknowledgement Message “file upload to server successfully”



To : amuser311@gmail.com

From Date : Ved 01/30/2019 From Time : 17:27 PM To Date : Thu 01/31/2019 To Time : 17:12 PM

What is Accounting?
Accounting is the process of systematically recording, measuring, and communicating information about financial transactions.

How does Accounting work?
At the heart of accounting is the double-entry bookkeeping method. This involves making at least two recording entries for every transaction: a debit in one account and a credit in another account. The method helps prevent errors because the sum of the debits should equal the sum of the credits. The three major financial statements produced by accounting are the income statement, the balance sheet, and the cash flow statement.

Accounting can be done on a cash basis (cash accounting) or on an accrual basis (accrual accounting). Cash accounting records cash inflows and outflows in the period in which they

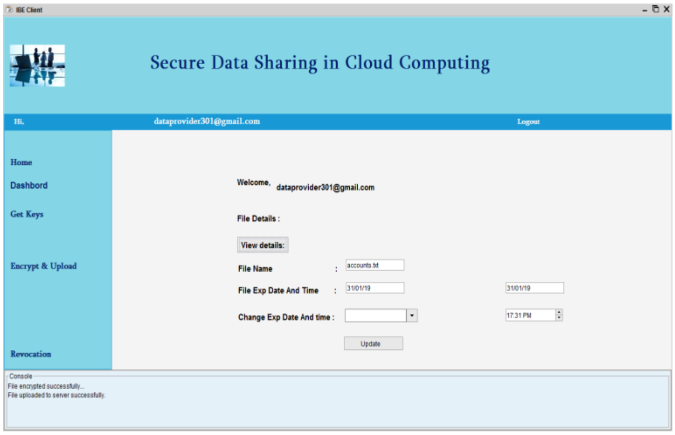
File name:-accounts.txt

File Hash computation data:-
c7486cd7c9c2352cb67a9d3c8a8d32f7b489399d

Console
File encrypted successfully...
File uploaded to server successfully.

On dashboard of data provider ,shared file information is display with time stamp.

If data provider want to extend timestamp He/she can extend by clicking on" **Change exp date and time**",and submit on clicking update button



Welcome, dataprovider301@gmail.com

File Details :

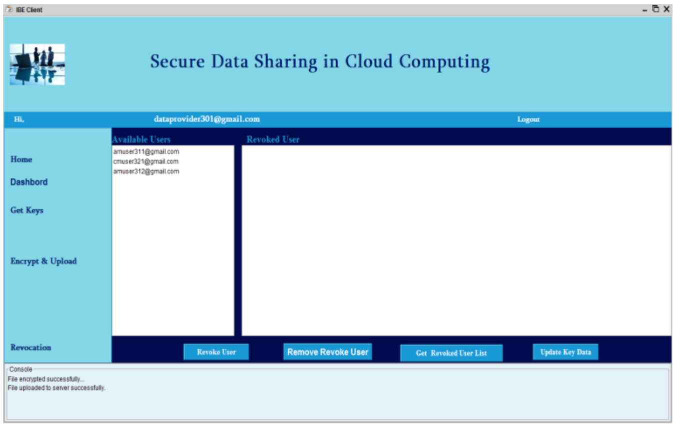
File Name : accounts.txt

File Exp Date And Time : 31/01/19 31/01/19

Change Exp Date And time : 17:31 PM

Console
File encrypted successfully...
File uploaded to server successfully.

10. Revocation Tab

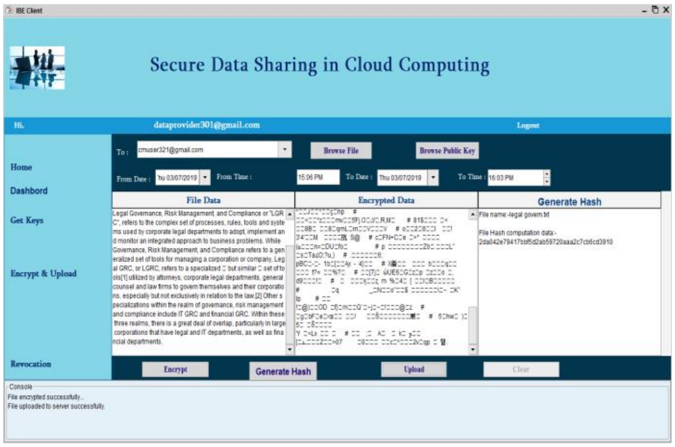


amuser311@gmail.com
cmuser321@gmail.com
amuser312@gmail.com

Console
File encrypted successfully...
File uploaded to server successfully.

Sec II

1. Data Provider share File "Legal govern" with CM user for timestamp : Thursday 7/3/19(15:06 PM to 16:06 PM)



To : cmuser321@gmail.com

From Date : 'hu 03/07/2019 From Time : 15:06 PM To Date : Thu 03/07/2019 To Time : 16:03 PM

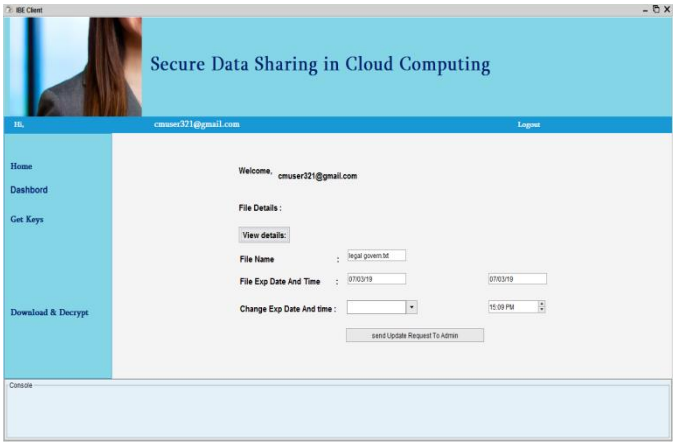
Legal Governance, Risk Management, and Compliance or "LGRC", refers to the complex set of processes, rules, tools and systems used by corporate legal departments to adopt, implement and monitor an integrated approach to business problems. While Governance, Risk Management, and Compliance refers to a generalized set of tools for managing a corporation or company, Legal GRC, or LGRC, refers to a specialized but similar set of tools[1] utilized by attorneys, corporate legal departments, general counsel and law firms to govern themselves and their corporations, especially but not exclusively in relation to the law.[2] Other specializations within the realm of governance, risk management and compliance include IT GRC and financial GRC. Within these three realms, there is a great deal of overlap, particularly in large corporations that have legal and IT departments, as well as financial departments.

File name:-legal govern.txt

File Hash computation data:-
2da042e79417bbf5d2ab59720aaa2c7cb6cd3910

Console
File encrypted successfully...
File uploaded to server successfully.

1. CM User Dashboard


IBE Client
Secure Data Sharing in Cloud Computing
Hi, cmuser321@gmail.com Logout
Home
Dashbord
Get Keys
Download & Decrypt
View details:
send Update Request To Admin
Console

Welcome, cmuser321@gmail.com

File Details :

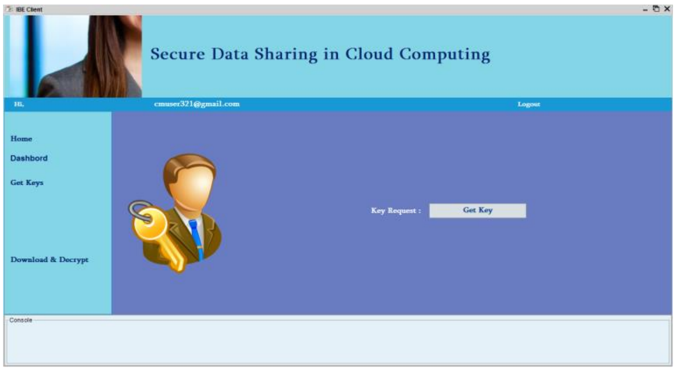
File Name : legal govern.txt

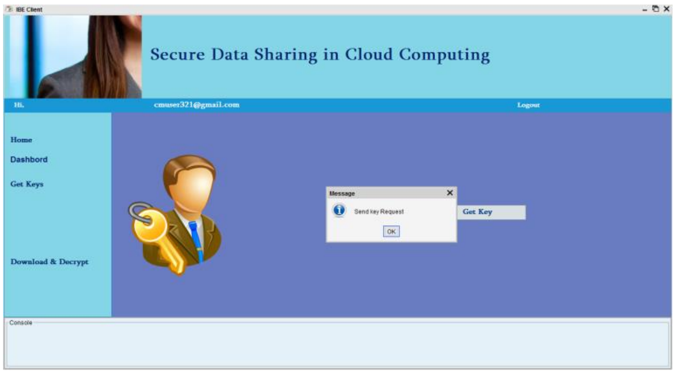
File Exp Date And Time : 07/03/19 07/03/19

Change Exp Date And time : 15:09 PM

CM user will Request to Key Distributer for downloading Shared file

Getkey

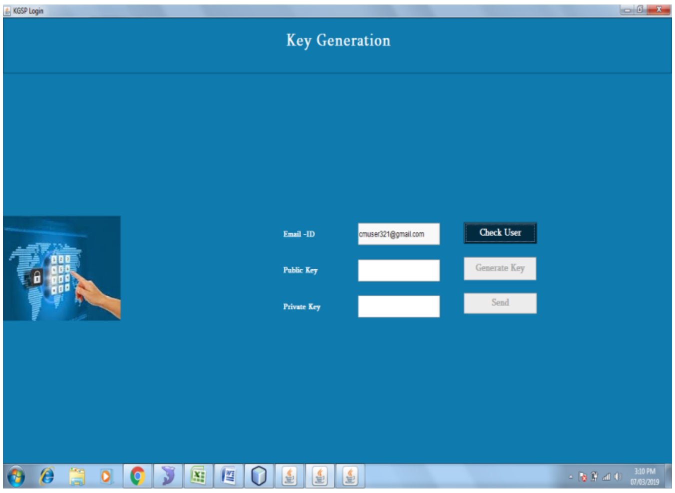




cmuser321@gmail.com

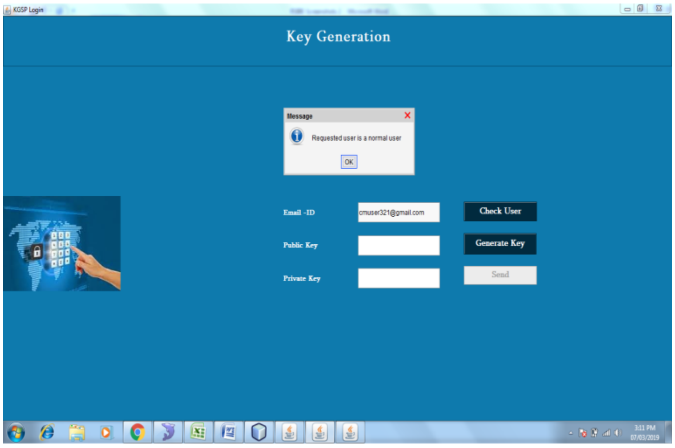
Send key Request

1. On Key Distributer Window : Request will appear like this



Email -ID: cmuser321@gmail.com

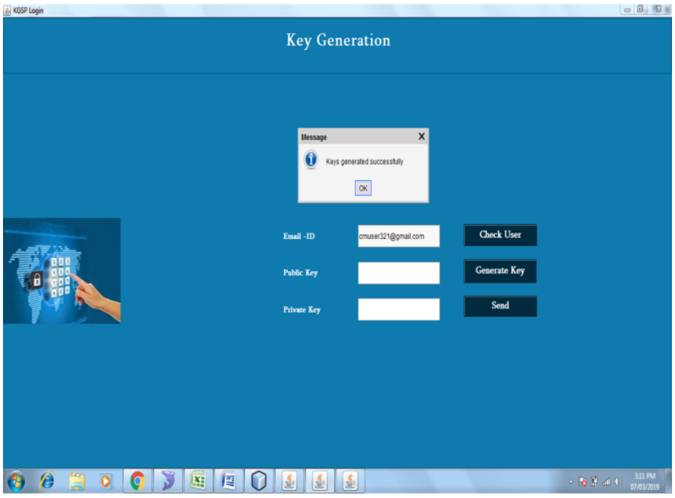
- After Click on **Check User** Button



Requested user is a normal user

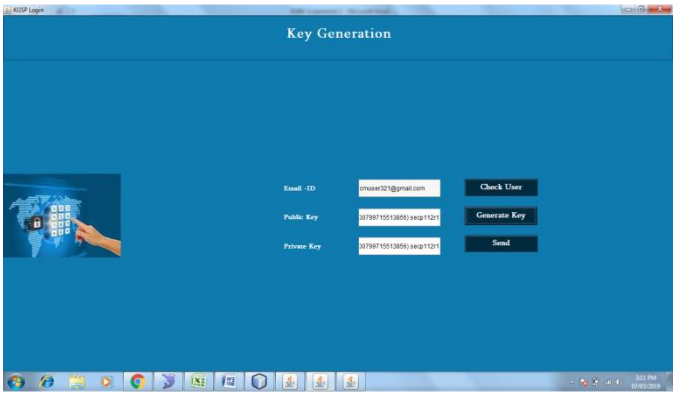
Email -ID: cmuser321@gmail.com

- After Click on **Generate Key** Button



Keys generated successfully

Email -ID: cmuser321@gmail.com

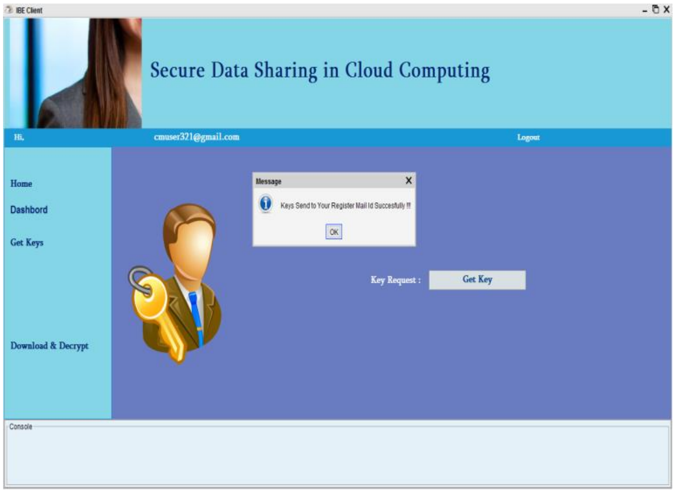


Email -ID: cmuser321@gmail.com

Public Key:)0799715513856) secp112r1

Private Key:)0799715513856) secp112r1

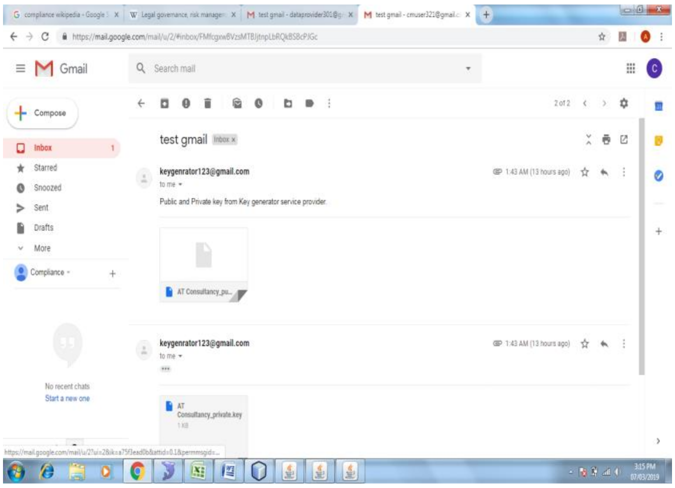
After send button



cmuser321@gmail.com

Keys Send to Your Register Mail Id Succesfully !!!

will send to register Email id , On CM User Gmail Window

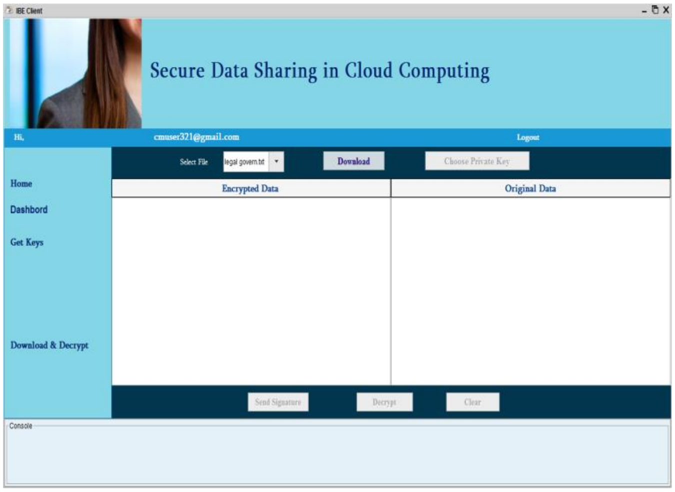


test gmail

keygenrator123@gmail.com
to me
Public and Private key from Key generator service provider.

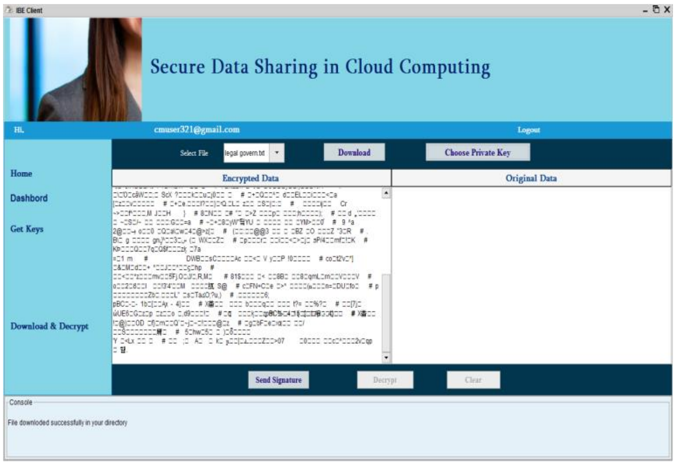
keygenrator123@gmail.com
to me

1. CM user will download key and Decrypt File using key **Download & Decrypt Tab**



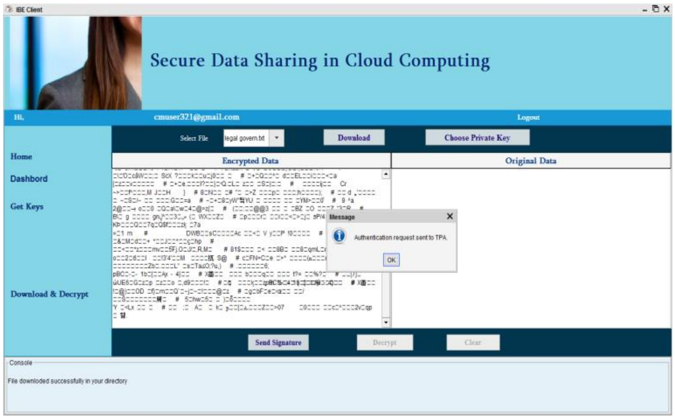
1. When CM user click on Download button then Encrypted File will download and CM will Choose Private key which is received on Gmail from Key Generator

2. When CM user will choose private key then **Send Signature** button will visible



File downloaded successfully in your directory

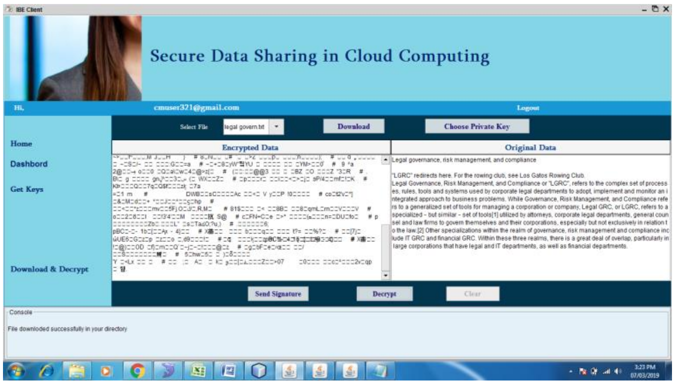
After clicking send Signature Button . Message box will Appear : ***Authentication request send to TPA***



Authentication request sent to TPA

File downloaded successfully in your directory

After challenge response ,CM will Successfully decrypt file

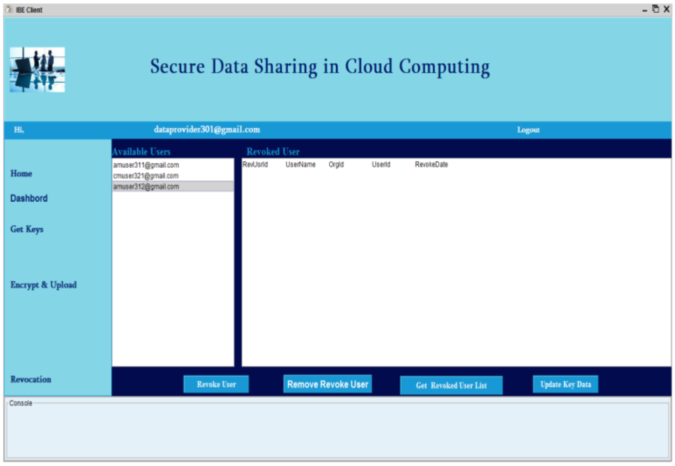


Legal governance, risk management, and compliance

"LGRC" redirects here. For the rowing club, see Los Gatos Rowing Club.
Legal Governance, Risk Management, and Compliance or "LGRC", refers to the complex set of processes, rules, tools and systems used by corporate legal departments to adopt, implement and monitor an integrated approach to business problems. While Governance, Risk Management, and Compliance refers to a generalized set of tools for managing a corporation or company, Legal GRC, or LGRC, refers to a specialized - but similar - set of tools[1] utilized by attorneys, corporate legal departments, general counsel and law firms to govern themselves and their corporations, especially but not exclusively in relation to the law.[2] Other specializations within the realm of governance, risk management and compliance include IT GRC and financial GRC. Within these three realms, there is a great deal of overlap, particularly in large corporations that have legal and IT departments, as well as financial departments.

File downloaded successfully in your directory

1. On Data Provider Window ***Revocation*** Tab is look like this



Available Users:

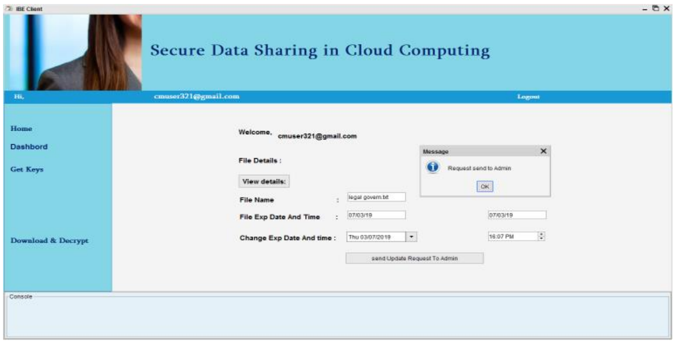
amuser311@gmail.com
cmuser321@gmail.com
amuser312@gmail.com

RevUsrId	UserName	OrgId	UserId	RevokeDate

1. **ON CM User Window**

   Legal Govern File is shared With CM User for timestamp 7/3/19 (15:06PM to 16:06PM)

   User can renew expiry date by requesting to data provider.



cmuser321@gmail.com

Welcome, cmuser321@gmail.com

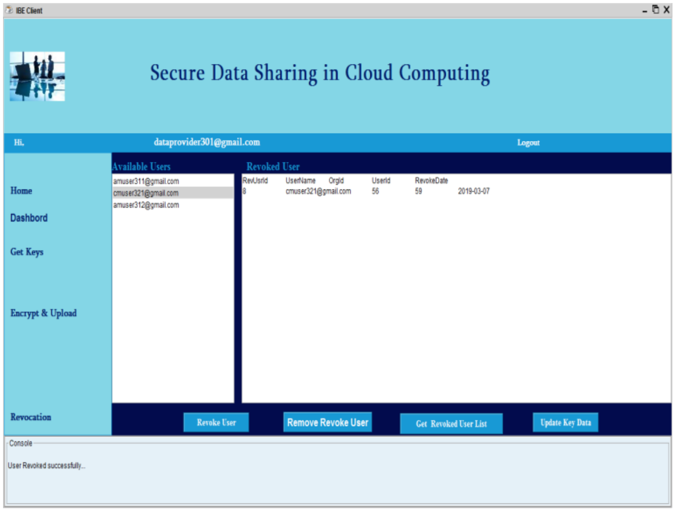
File Name : legal govern.txt

File Exp Date And Time : 07/03/19 07/03/19

Change Exp Date And time : Thu 03/07/2019 16:07 PM

Request send to Admin

1. ON Data Provider Window **After timestamp expire** , Data Provider Revocation Window



Available Users:

amuser311@gmail.com
cmuser321@gmail.com
amuser312@gmail.com

RevUsrId	UserName	OrgId	UserId	RevokeDate	
8	cmuser321@gmail.com		56	59	2019-03-07

User Revoked successfully...

4.. RESULTS

So according to experiments execution it support identity revocation and cipher text update simultaneously such that a revoked user is prevented from accessing previously shared data, as well as subsequently shared data.

5.CONCLUSION

In this paper we conclude Cloud computing brings great benefits for people. Particularly, it perfectly matches the increased need of sharing data over the Internet. There is need of privacy security with access control for sharing data. Considering this we present cost effective and secure data sharing system in cloud computing called Revocable- Storage Identity-Based Encryption (RS-IBE) which fulfills the security goals i.e. data confidentiality, Backward secrecy, Forward secrecy and it also supports identity revocation and cipher text update simultaneously such that a revoked user is prevented from accessing previously shared data, as well as subsequently shared data. We analyze the performance of scheme in terms of efficiency & functionality and make it more feasible for practical application.

6.REFERENCES

[1]A. Shamir, "Identity-based cryptosystems and signature schemes ,"in *Advances in cryptology*.

[2] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," *SIAM Journal on Computing*, vol. 32, no. 3, pp. 586–615, 2003

[3] C. Gentry, "Certificate-based encryption and the certificate revocation problem," in *Advances in Cryptology–EUROCRYPT 2003*. Springer, 2003.

[4] A. Boldyreva, V. Goyal, and V. Kumar, "Identity-based encryption with efficient revocation," in *Proceedings of the 15th ACM conference on Computer and communications security*. ACM, 2008, pp. 417–426.

[5] B. Libert and D. Vergnaud, "Adaptive-id secure revocable identity based encryption," in *Topics in Cryptology–CT-RSA 2009*. Springer,2009, pp. 1–15.