ISSN XXXX XXXX © 2017 IJESC

Research Article Volume 7 Issue No.6

Flexible and Fine-Grained Attribute-Based Data Storage in Cloud Computing

Pramod .P[1], Prof. H. R. Divakar[2]
PG Scholar[1], Assistant Professor[2]
Department of MCA
PES College of Engineering, Mandya, Karnataka, India

Abstract:
"FELXIBLE AND FINE GRAINED ATTRIBUTE BASED DATA STORAGE IN CLOUD COMPUTING" The development of cloud computing, outsourcing data to cloud server attracts lots of attentions. To guarantee the security and achieve flexibly fine-grained file access control, attribute based encryption (ABE) was proposed and used in cloud storage system. However, user revocation is the primary issue in ABE schemes. In this article, we provide a cipher text-policy attribute based encryption (CP-ABE) scheme with efficient user revocation for cloud storage system. The issue of user revocation can be solved efficiently by introducing the concept of user group. When any user leaves, the group manager will update users' private keys except for those who have been revoked. Additionally, CP-ABE scheme has heavy computation cost, as it grows linearly with the complexity for the access structure. To reduce the computation cost, we outsource high computation load to cloud service providers without leaking file content and secret keys. Notably, our scheme can withstand collusion attack performed by revoked users cooperating with existing users. We prove the security of our scheme under the divisible computation Diffie-Hellman (DCDH) assumption. The result of our experiment shows computation cost for local devices is relatively low and can be constant. Our scheme is suitable for resource constrained devices.

I. INTRODUCTION

Cloud computing, as a new technology paradigm with promising further, is becoming more and more popular nowadays. It can provide users with seemingly unlimited computing resource. Enterprises and people can outsource time consuming computation workloads to cloud without spending the extra capital on deploying and maintaining hardware and software. Flexibly and fine-grained file access control, attribute based encryption (ABE) was proposed and used in cloud storage system. However, user revocation is the primary issue in ABE schemes. In this article, we provide a cipher text policy attribute based encryption (CP-ABE) scheme with efficient user revocation for cloud storage system. The issue of user revocation can be solved efficiently by introducing the concept of user group. When any user leaves, the group manager will update users' private keys except for those who have been revoked. Security issues are main obstacles for wide application of cloud computing .To achieve flexible fine-grained file access control, attribute based encryption (ABE) was proposed and used. However, user revocation is the primary issue in ABE schemes. We need efficient user revocation for cloud storage system. At the same time heavy computation cost should not spoil the application performance. The system should with stand collusion attack performed by revoked users cooperating with existing users. The system should be suitable for resource constrained devices also. CP-ABE scheme has heavy computation cost, as it grows linearly with the complexity for the access structure. To reduce the computation cost, we outsource high computation load to cloud service providers without leaking file content and secret keys. Notably, our scheme can withstand collusion attack performed by revoked users cooperating with existing users. We prove the security of our scheme under the divisible computation Diffie-Hellman (DCDH) assumption. The result of our experiment shows computation cost for local devices is relatively low and can be constant. Our scheme is suitable for resource constrained devices. A basic CP-ABE scheme concludes the following fundamental algorithms:

Setup: This algorithm takes a security parameter as input. It outputs a public parameter and a master key.

Encrypt: This algorithm takes the public parameter, a message, and an access policy in the attribute universe as input. The algorithm outputs a cipher-text CT such that only the user whose attribute set satisfies the access policy can decrypt

Key Gen: This algorithm takes the master key and an attribute set as input. It outputs a private key with respect to the attribute set.

Decrypt: This algorithm takes the public parameter, a cipher-text CT, and a private key as input. If the user's attribute set satisfies the access structure embedded in the Cipher-Text, then the algorithm decrypts the cipher-text successfully Perform user revocation operation by combining CP-ABE with re-encryption. In their scheme, each user belongs to a group and holds a group secret key issued by the group Manager.

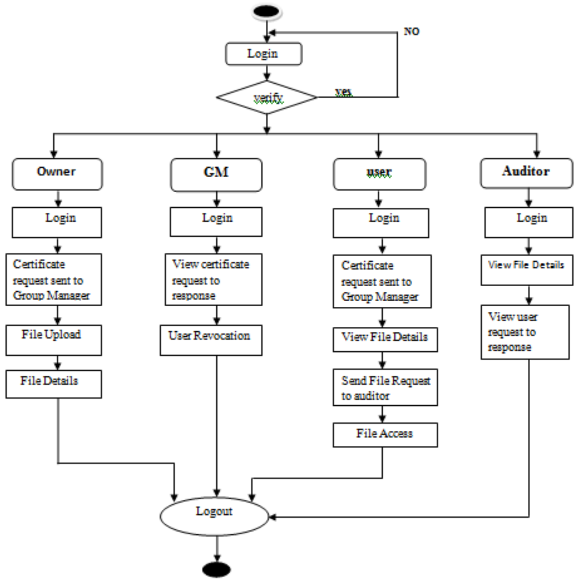
The main contributions in this project are as follows

- In this system, we focus on designing a CP-ABE scheme with efficient user revocation for cloud storage system.
- We aim to model collusion attack performed by revoked users cooperating with existing users.
- Furthermore, we construct an efficient user revocation CP-ABE scheme through improving the existing scheme and prove our scheme is CPA secure under the selective model.
- To solve existing security issue, we embed a certificate into each user's private key. In this way, each user's group secret key is different from others and bound together with his private key associated with attributes.
- To reduce users' computation burdens, we introduce two cloud service providers named encryption-cloud service provider (E-CSP) and decryption-cloud service provider (D-CSP).

- The duty of E-CSP is to perform outsourced encryption operation and D-CSP is to perform outsourced decryption operation.
- In the encryption phase, the operation associated with the dummy attribute is performed locally while the operation associated with the sub-tree is outsourced to E-CSP.

Activity Diagram

Activity diagrams are graphical representations of workflows of stepwise activities and actions with support for choice, iteration and concurrency. In the Unified Modelling Language, activity diagrams can be used to describe the business and operational step-by-step workflows of components in a system. An activity diagram shown in Figure 1



Login
NO
verify
yes
Owner
GM
user
Auditor
Login
Login
Login
Login
Certificate request sent to Group Manager
View certificate request to response
Certificate request sent to Group Manager
View File Details
File Upload
User Revocation
View File Details
View user request to response
File Details
Send File Request to auditor
File Access
Logout

Figure.1.Activity Diagram

IMPLEMENTATION

The application consists of four modules Data Owner, Data User, Group Manager and Auditor. Each module has several role. These roles are explained through activity diagram. The flow of the work as follows in Figure 2

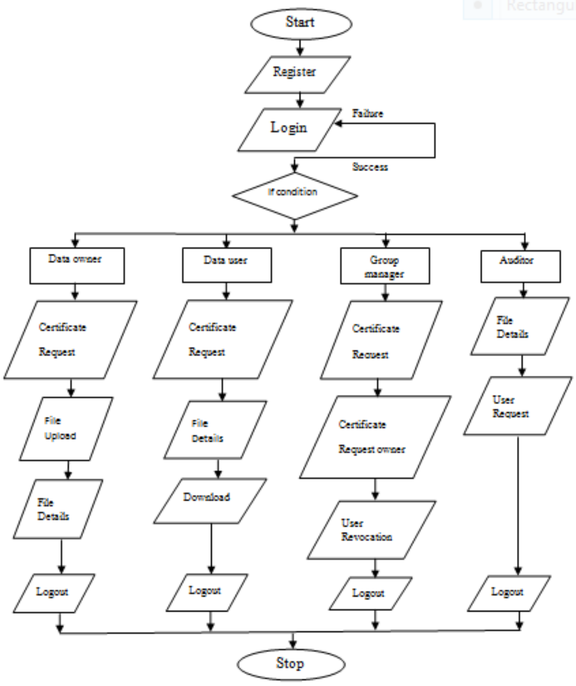
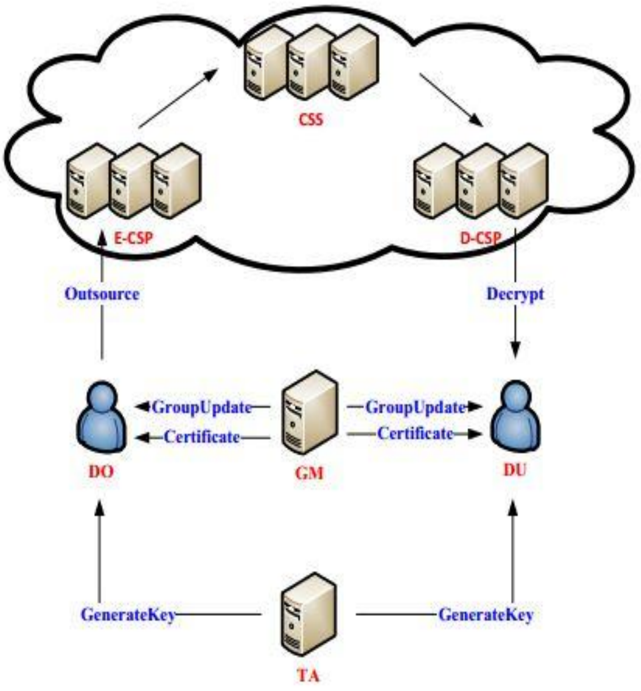


Figure. 2.FlowChart

II.SYSTEM ARCHITECTURE



III.NON – FUNCTIONAL REQUIREMENTS

Non – Functional requirements, as the name suggests, are those requirements that are not directly concerned with the specific functions delivered by the system. They may relate to emergent system properties such as reliability response time and store occupancy. Alternatively, they may define constraints on the system such as the capability of the Input Output devices and the data representations used in system interfaces. Many non-functional requirements relate to the system as whole rather than to individual system features. This means they are often critical than the individual functional requirements. The following non-functional requirements are worthy of attention.

The key non-functional requirements are:

1) **Security:** The system should allow secure communication between cloud server & user.

2) **Platform Independence:** The application should run on any platform without recompilation.

3) **Reliability:** The system should be reliable and must not degrade the performance of the existing system and should not lead to the hanging of the system.

4) **Response time**: The application response time should be quick.

5) **Scalability:** The system should provide optimal performance even if the user base grows dramatically.

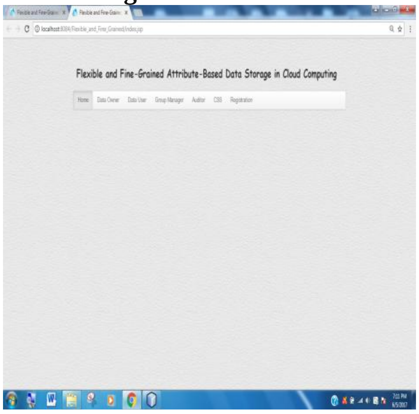
6) **Maintainability:** The system should support incorporation of future requirements easily.

7) **Robustness**: The application should be fault tolerant with respect to illegal user/receiver inputs. Error checking has been built in the system to prevent system failure.

IV. RESULTS AND DISCUSSION

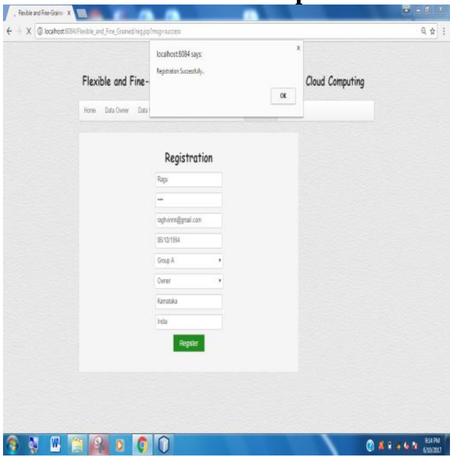
This Project is developed by using core java it is used for Implementing business logic, with a backend database is MYSQL and JSP it is used for creating Dynamic web pages and a web browser and the servlet it is used for controller to control the flow of application. This implementation technologies such as JSP, programming language such as JAVA, JavaScript, and HTML ,relational databases MySQL, Access.

1.Home Page


localhost:8084/Flexible_and_Fine_Grained/index.jsp

Flexible and Fine-Grained Attribute-Based Data Storage in Cloud Computing

2.Data Owner Relationship


localhost:8084/Flexible_and_Fine_Grained/reg.jsp?msg=success

localhost:8084 says:

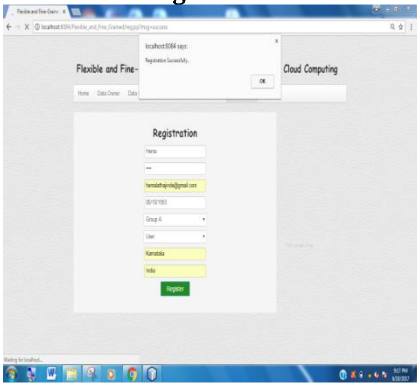
Registration Successfully..

Flexible and Fine- Cloud Computing

Registration

Ragu
***
raghvinnn@gmail.com
06/10/1994
Group A
Owner
Karnataka
India

3.Data User Registration


localhost:8084/Flexible_and_Fine_Grained/reg.jsp?msg=success

localhost:8084 says:

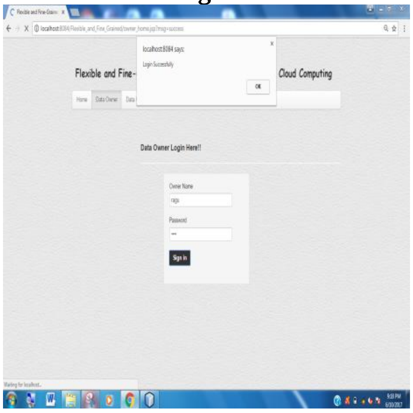
Registration Successfully..

Flexible and Fine- Cloud Computing

Registration

Hema
***
hemalathajinde@gmail.com
06/10/1993
Group A
User
Karnataka
India

4.Data Owner Login


localhost:8084/Flexible_and_Fine_Grained/owner_home.jsp?msg=success

localhost:8084 says:

Login Successfully

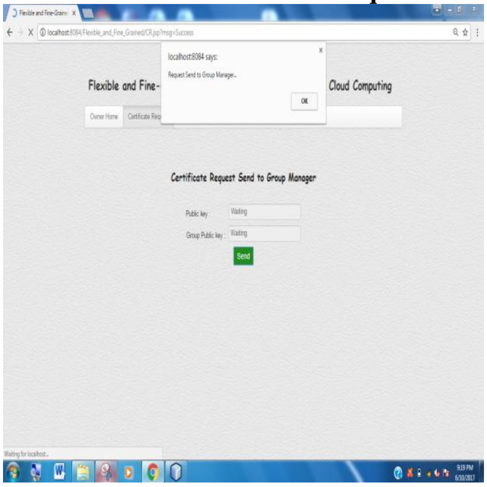
Flexible and Fine- Cloud Computing

Data Owner Login Here!!

Owner Name: ragu

Password: ***

5.Data owner send certificate request to GM


localhost:8084/Flexible_and_Fine_Grained/CR.jsp?msg=Success

localhost:8084 says:

Request Send to Group Manager...

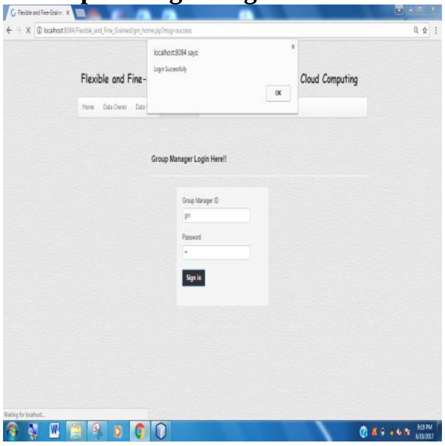
Flexible and Fine- Cloud Computing

Certificate Request Send to Group Manager

Public key : Waiting

Group Public key : Waiting

6.Group Manager Login


localhost:8084/Flexible_and_Fine_Grained/gm_home.jsp?msg=success

localhost:8084 says:

Login Successfully

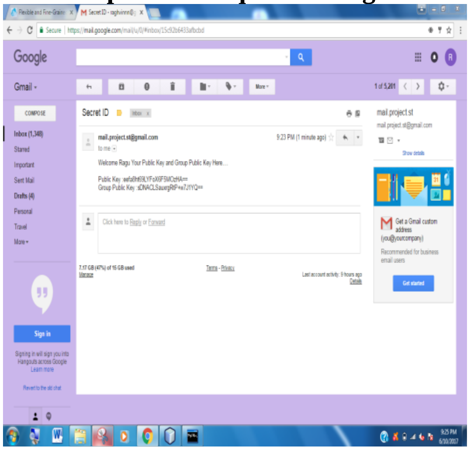
Flexible and Fine- Cloud Computing

Group Manager Login Here!!

Group Manager ID: gm

Password: **

7.GM response to request through Mail Id


https://mail.google.com/mail/u/0/#inbox/15c92b6433afbcbd

Secret ID

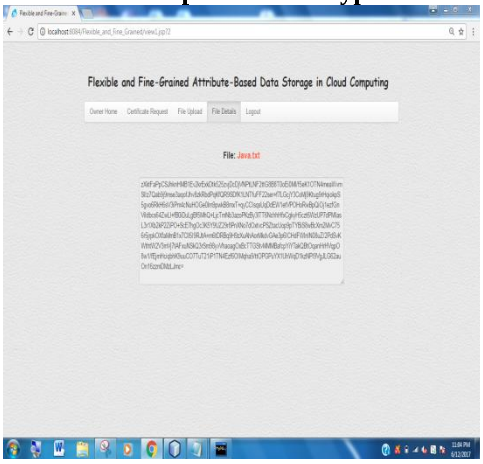
mail.project.st@gmail.com 9:23 PM (1 minute ago)
to me

Welcome Ragu Your Public Key and Group Public Key Here....

Public Key :eefa8ht69LYFoX6F5MOzHA==
Group Public Key :sDNACLSauxgRtP+w7J1YQ==

Google
Gmail
More
1 of 5,201
COMPOSE
Inbox (1,348)
Starred
Important
Sent Mail
Drafts (4)
Personal
Travel
More
Inbox
mail.project.st
mail.project.st@gmail.com
Show details
Click here to Reply or Forward
7.17 GB (47%) of 15 GB used
Manage
Terms - Privacy
Last account activity: 9 hours ago
Details
Get a Gmail custom address (you@yourcompany)
Recommended for business email users
Get started
Sign in
Signing in will sign you into Hangouts across Google
Learn more
Revert to the old chat

8.Data Owner upload In Encryption Form

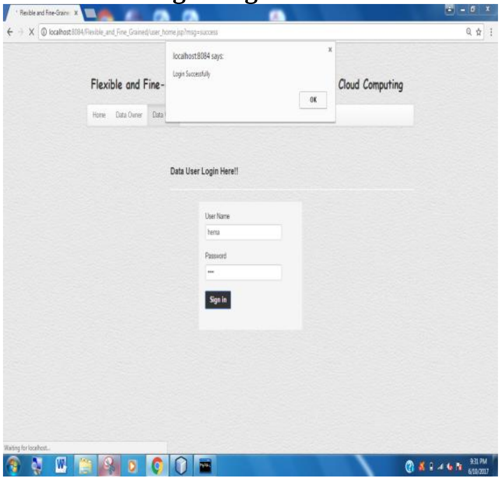

localhost:8084/Flexible_and_Fine_Grained/view1.jsp?2

Flexible and Fine-Grained Attribute-Based Data Storage in Cloud Computing

File: Java.txt

```
zXktFaPpCSJhknHMB1Ev2krExkOtk525zvjDcDjVNPtLNF2ttG8B6T0oE0Ml15eK1OTN4meaWvm
5lz7Qab6j9mse3aqofJhv8zkRbdPqKfQR9SDfK1LNT1uFF22ser+t7LGcjY3CoMj9KtugfrHqokpS
5gvo6RkH6sV3iPm4cNuHOGe0In9pwkB8mxT+qyCCIsqsUqDdEW1etVPOHoRwBpQiOj1ezfGn
Vkdbcs64ZwLI+fB0iDuLgBf5MhQ+LjcTmNb3azsPKzBy3lTT6NchhHfxCgkyH5czt6WzUP7dPMas
L3r1Xb2kP2ZiPO+ScE7hgOc3K5Y9UZ29r8PnXNo7dOxtvcPSZtacUop9pTYBiS8wBcXm2MvC75
6r5jqpkOXfaMrnB1x7Cl6i9RJtA+m6tDRBq9H9zXuAhAorMkdvGAe3p6iCHdFWlnN08uZ/2PdSvK
WtttW2V3mMj7tAFxuN9kQ3rSm98yVhaoagOxBcTTGStvMMMBafcpYiYTakQBtOqanHrHVqpO
8w1fEjmHoxjbhK9uuCOTTuT21lP1TN4Ez6OlMqha9ttOPGPvYX1UhWqD1kzNPt9VgJLG62au
On16zmDNzLJmc=
```

9.Data User Login Page



localhost:8084 says:

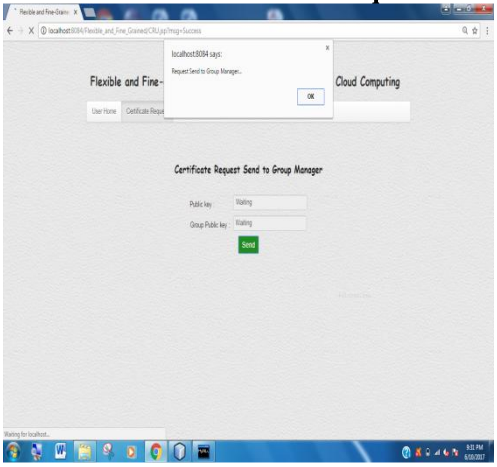
Login Successfully

Data User Login Here!!

User Name: hema

Password: ***

10.Data User send certificate Request to GM& Auditor



localhost:8084 says:

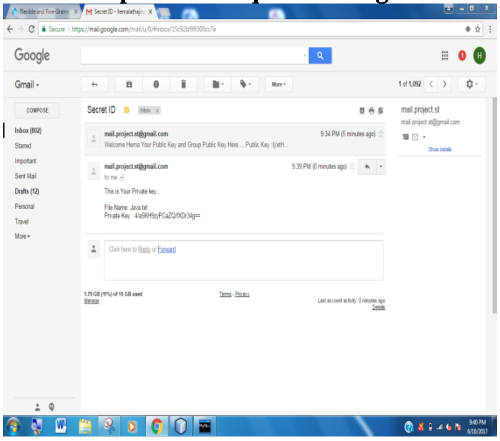
Request Send to Group Manager...

Certificate Request Send to Group Manager

Public key: Waiting

Group Public key : Waiting

11.GM response to request through User Mail Id



Secret ID Inbox

mail.project.st@gmail.com 9:34 PM (5 minutes ago)
Welcome Hema Your Public Key and Group Public Key Here.... Public Key :I/xtH...

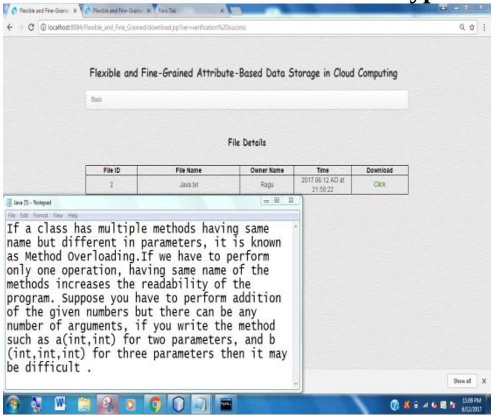
mail.project.st@gmail.com 9:39 PM (0 minutes ago)
to me

This is Your Private key...

File Name :Java.txt
Private Key : 4/a5KH9zyPCaZQ/fXDr34g==

Click here to Reply or Forward

12.Data User Download File in Decryption form


Flexible and Fine-Grain
Flexible and Fine-Grain
New Tab
localhost:8084/Flexible_and_Fine_Grained/download.jsp?ver=verification%20success
Back
Java (5) - Notepad
File Edit Format View Help
9:40 PM
6/10/2017

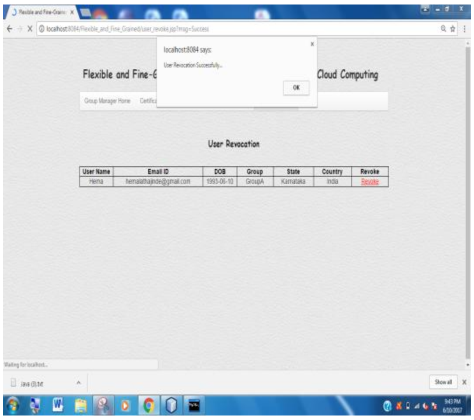
Flexible and Fine-Grained Attribute-Based Data Storage in Cloud Computing

File Details

File ID	File Name	Owner Name	Time	Download
2	Java.txt	Ragu	2017.06.12 AD at 21:50:22	Click

```
If a class has multiple methods having same
name but different in parameters, it is known
as Method Overloading.If we have to perform
only one operation, having same name of the
methods increases the readability of the
program. Suppose you have to perform addition
of the given numbers but there can be any
number of arguments, if you write the method
such as a(int,int) for two parameters, and b
(int,int,int) for three parameters then it may
be difficult .
```

13.GM has Revoked User



localhost:8084 says:

User Revocation Successfully...

User Revocation

User Name	Email ID	DOB	Group	State	Country	Revoke
Hema	hemalathajinde@gmail.com	1993-06-10	GroupA	Karnataka	India	Revoke

IV.CONCLISION

We provided a formal definition and security model for CP-ABE with user revocation. We also constructed a concrete CP-ABE scheme which is CPA secure based on DCDH assumption. To resist collusion attack, we embed a certificate into the user's private key. So that malicious users and the revoked users do not have the ability to generate a valid private key through combining their private keys. Additionally, we outsource operations with high computation cost to reduce the user's computation burdens. Through applying the technique of outsource, computation cost for local devices is much lower and relatively fixed. The results of our experiment show that our scheme is efficient for resource constrained devices.

V.FUTURE ENHANCEMENTS

1. Better algorithm than CP-ABE can be designed to improve the performance.
2. UI can be improved

3. Private key can be sent to mobile phone

4. Data leakage detection mechanism can be implemented

V.REFERENCES

Reference Books

[1]. Paul C Jagerson, “Software Testing”, Craftsmen’s Edition, 2007

[2]. Herbert Schildt, “Java Complete reference”, Tata McGraw Hill

[3]. Roger.S. Pressman,” SOFTWARE ENGINEERING”, MCGRAW HILL 6th, Edition 2005.

[4]. Sommerville, “Ian (2011) Software Engineering”, Addison-Wesley, Boston, MA.

[5]. J.Bethencourt, A.Sahaiand B.Waters, “Ciphertext-Policy Attribute- Based Encryption

[6]. Boldyreva, V. Goyal, and V. Kumar, “Identity-Based En-cryption with Efficient Revocation