**IJCTA**, 9(24), 2016, pp. 9-16 ISSN: 0974-5572
© International Science Press

# Organized and Protected Communication in Mobile Group

**D. Saravanan***

**ABSTRACT**

In this Paper, an Efficient and Secure User Revocation Scheme in Mobile Social Networks has been proposed where each user is connected extensively with his/her social friends or others users sharing similar interests. Scope of the Paper is that it describes a family of key management algorithms that reduce the cost due to multiple user revocation while keeping the storage cost manageable.

***Key Terms:*** Data Communication, Encryption, Decryption, Secret Key, Group Key, Communication, Confidentiality.

## 1. INTRODUCTION

It is necessary to secure the group communication as the data are sensitive or it requires the users to pay for it. In the algorithms for secure group communication a group key is shared by all the users. The group key is used to encrypt data transmitted to the group. The group membership is dynamic. When group membership changes, to protect the confidentiality of the current users, a new group key needs to be shared by the users. When a user is admitted to the group, the group controller changes the group key and securely unit casts it to the joining user. To send the new group key to the current users, the group controller encrypts it with the old group key and multicasts it to them. Thus, the cost of rekeying for the group controller, due to a joining user is small.

However, when a user is revoked, i.e., the user leaves or is forcefully removed from the group, the group controller needs to securely uni cast the new group key to each of the remaining users. Toward this, the group controller encrypts the new group key with the personal keys of each of the remaining users and uni casts each message to the respective user. The cost of this process is symmetric key encryptions and messages. Thus, for a large group, revoking users from the secure group is an expensive operation. In these solutions, for a group of N users, the group controller distributes the new group key in encrypted messages. We note that in these solutions, the rekeying cost, i.e., number of encryptions performed and messages transmitted by the group controller, for a joining user is increased. However, techniques suggested in reduce the join cost to nearly constant and as such have been used by other approaches. On the other hand, the cost for revoking a user is reduced encrypted messages.

### 1.1. Existing System

- When a user is admitted to the group, the group controller changes the group key and securely uni casts it to the joining user.
- To send the new group key to the current users, the group controller encrypts it with the old group key and multicasts it to them. Thus, the cost of rekeying for the group controller, due to a joining user is small.
- However, when a user is revoked, i.e., the user leaves or is forcefully removed from the group, the group controller needs to securely unicast the new group key to each of the remaining users.

[*] Faculty of Operations & IT, IFHE University, IBS Hyderabad.

- The group controller encrypts the new group key with the personal keys of each of the remaining users and uni casts each message to the respective user.
- The cost of this process is symmetric key encryptions and messages. Thus, for a large group, revoking users from the secure group is an expensive operation.

#### *1.1.1. Disadvantages*

- Expensive operation of the Storage maintenance.
- The Group Controller needs to interrupt the Group Communication during the rekeying the resulting delay can be unreasonable for many applications.

### 1.2. Proposed System

- The goal of the Paper is to evaluate trade-off between storage and revocation cost. Storage is computed in terms of keys that each user (respectively, group controller) maintains.
- Revocation cost is computed in terms of the encryptions performed, and the number of messages transmitted, by the group controller.
- It describes a family of key management algorithms that reduce the cost due to multiple user revocation while keeping the storage cost manageable.
- It describes our family of key management algorithms for efficiently distributing the new group key when multiple users are revoked from the group.
- In Family of Key Management algorithms, the storage at the group controller is linear and the storage at the users is logarithmic in the size of the group.
- It describes techniques to reduce the number of keys stored by the users and the group controller.

#### *1.2.1. Advantages*

- Reduce the cost due to multiple user revocation while keeping the storage cost manageable.
- The Group Controller can efficiently distribute the Group Key.
- The Communication Overhead is only one message for revoking any number of users.

## 3. EXPERIMENTAL SETUP

Following are the modules which are used in Paper. They are given below:-

3.1 User Authentication

3.2 Group Controller

3.3 Key Generation

3.4 Encryption

3.5 Decryption

3.6 Key Update

### 3.1. User Authentication

It will identify the user and verify user to access.

### 3.2. Group Controller

The dynamics of the group membership can be handled under two settings. In the first setting, group controller manages the group membership and the users do not have the necessity to communicate among themselves. In the second setting, the group members collaborate by common group key. In this work, consider the first setting where a large group of users is managed by a group controller and consider the cost of membership handling in such applications.

### 3.3. Key Generation

Three key has been generated to ensure security. They are given below**:**

- ✓ Group key
- ✓ Secret key
- ✓ Share key

To ensure group security, all users in the group share a group key. The group key is used to encrypt the data transmitted to the group Secret key is a individual key given to particular nodes to exchange secret messages. A share key is generated when the nodes communicating the messages.

### 3.4. Encryption

In this module each node has a secret key (code) that it can use to encrypt information before it is sent over the network to another computer. Symmetric-key encryption is essentially the same as a secret code that each of the two computers must know in order to decode the information. The code provides the key to decoding the message.

### 3.5. Decryption

In this module all encrypted text converting it back into text that user and the computer are able to read and understand. To describe a method of un-encrypting the data manually or with un-encrypting the data using the proper codes or keys.

First user will registered in login form then the user window will open along with their members, The group control the group control and contained whole document and distribute the key to the users, which is internally done by the server. If any user leave from group then again group key on another user will changed when user communicate among the group then share key is used to multicast the data.

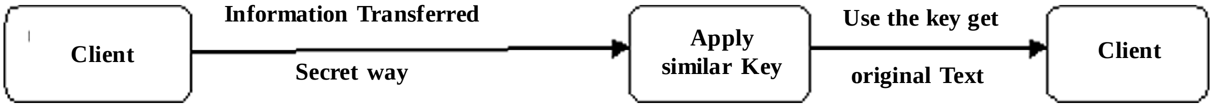


**Figure 1: Encryption**

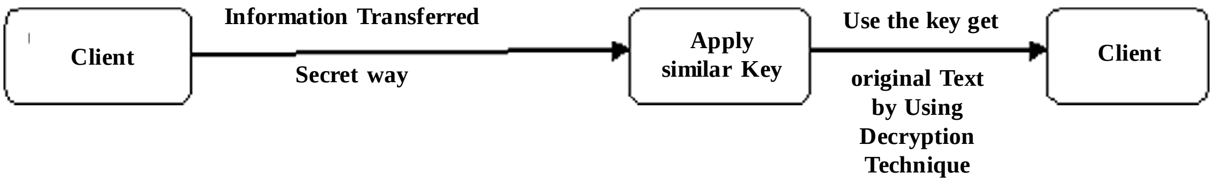


**Figure 2: Decryption**

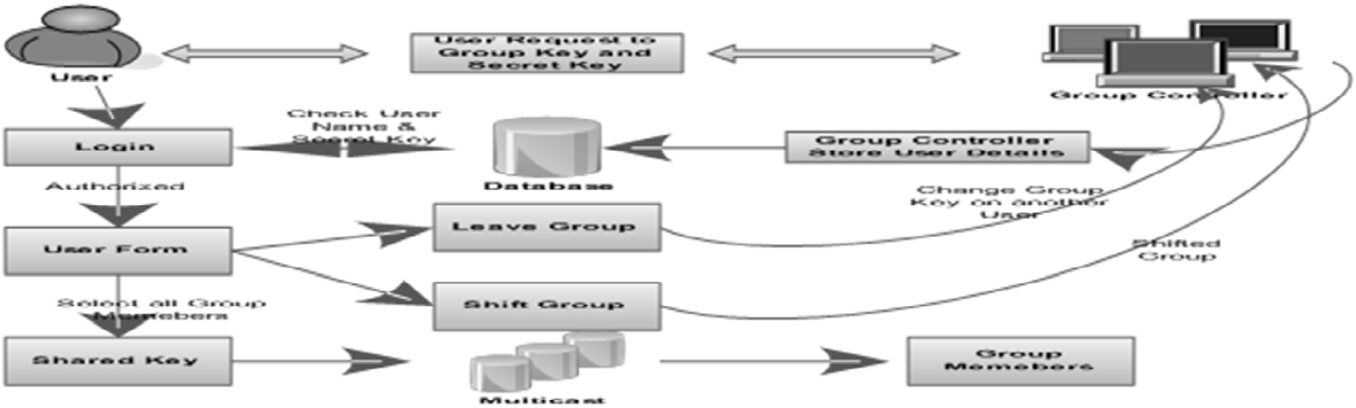

User
User Request to Group Key and Secret Key
Group Controller
Login
Check User Name & Secret Key
Database
Group Controller Store User Details
Authorized
User Form
Leave Group
Change Group Key on another User
Shifted Group
Shift Group
Select all Group Memebers
Shared Key
Multicast
Group Memebers

**Figure 3: System Flow Diagram**

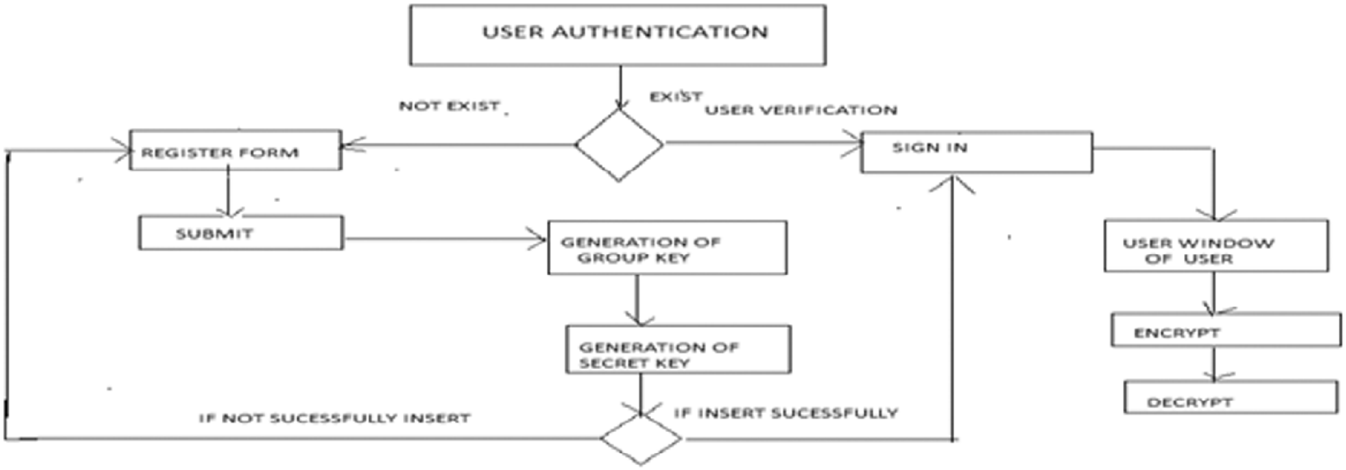


**Figure 4: Data Flow Diagram**

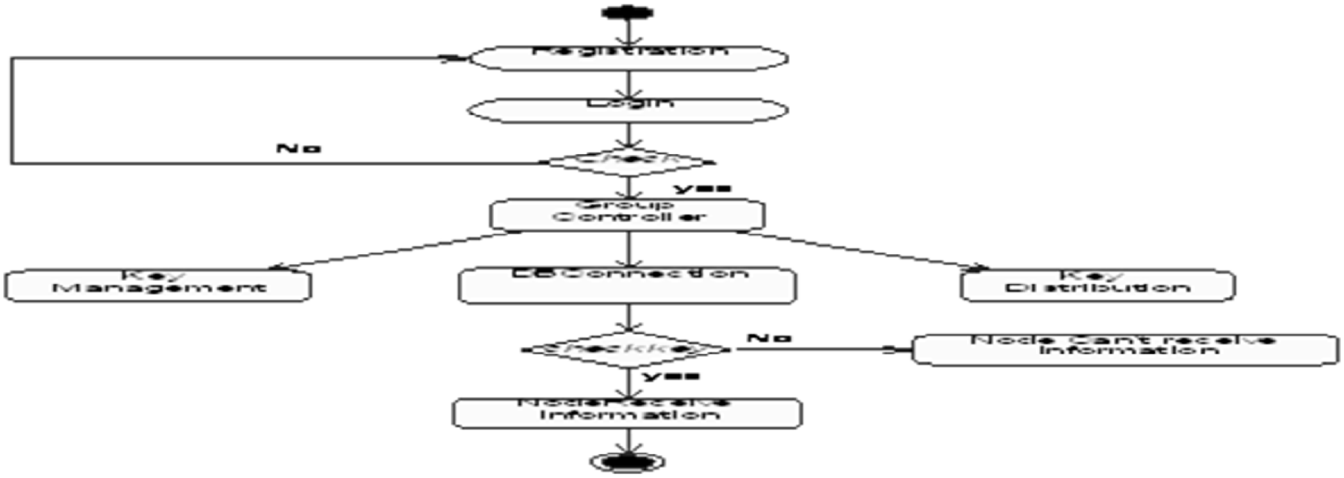


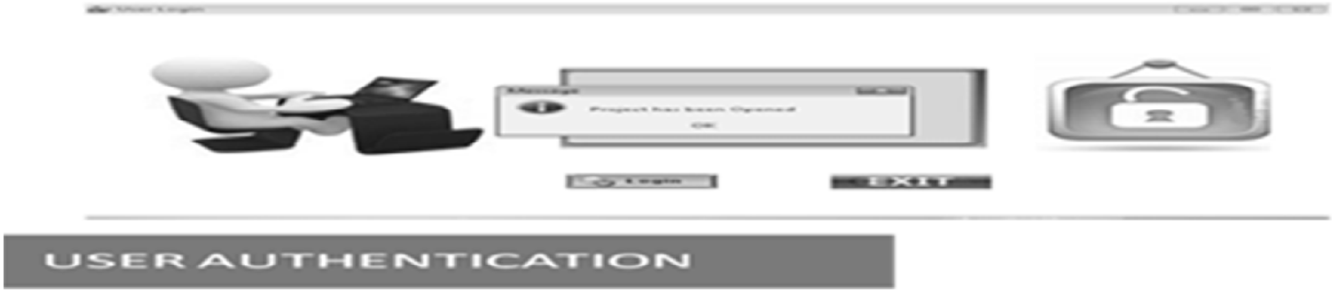
**Figure 5: Activity Diagram**

## 4. EXPERIMENTAL SETUP

Discussion: This screenshot is for entering into the Paper either. If server wants to access then server has to be entering the username along with password and these username and password should be correct then it will give the message "Paper has been opned".

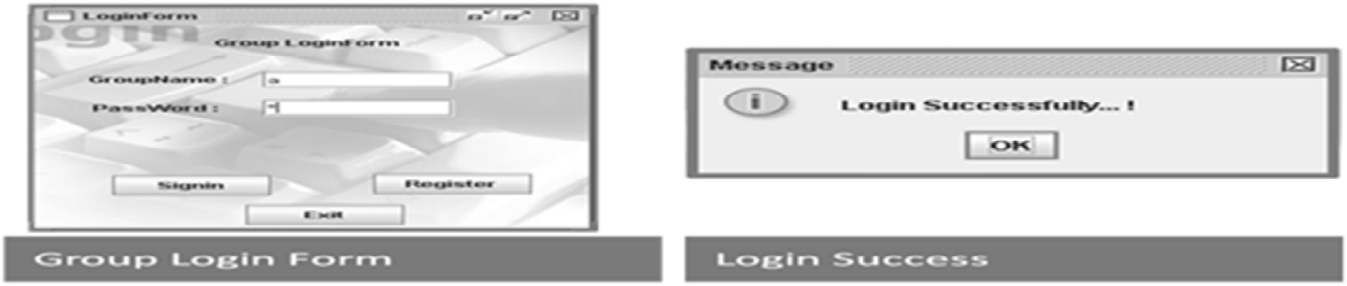
Discussion: This is group controller form to control all the groups'. Register a group to control

Discussion: After register the user registration form first server will generate the group key to secure the group.



Project has been Opened

**Figure 6: User Authentication**

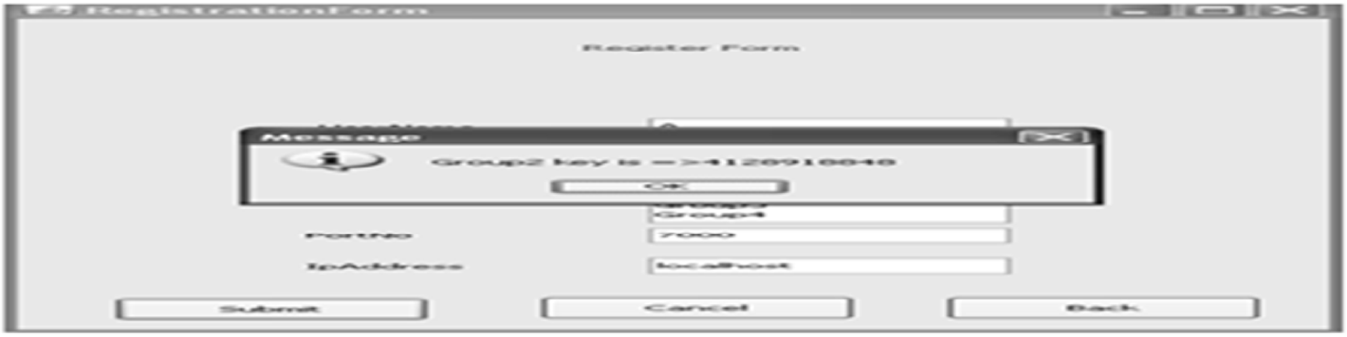


GroupName : a

PassWord : *

Login Successfully... !

**Figure 7: Group controller form**



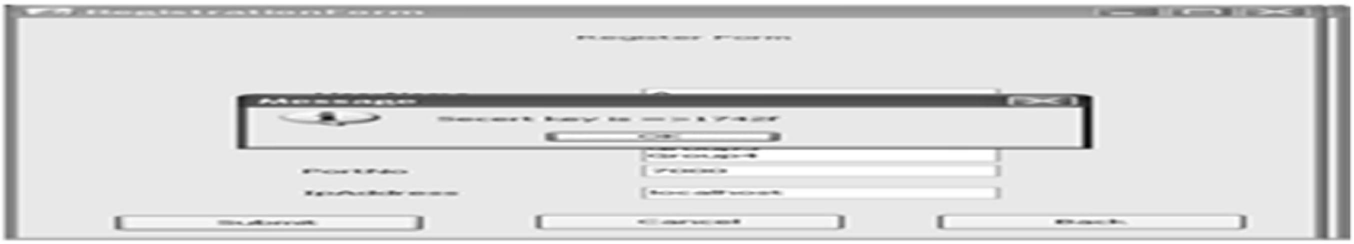
Group2 key is ==>4128918848

Group4

PortNo 7000

IpAddress localhost

**Figure 8: Group Key Generation**



Secret key is ==>1742f

Group4

PortNo 7000

IpAddress localhost

**Figure 9: Secret key Generation**

Discussion: This is the form for the users and secret is generated by the server for user only. This is personal key

Discussion: Data to be send is first encrypted and with the share key users will send the data to their selecting node.

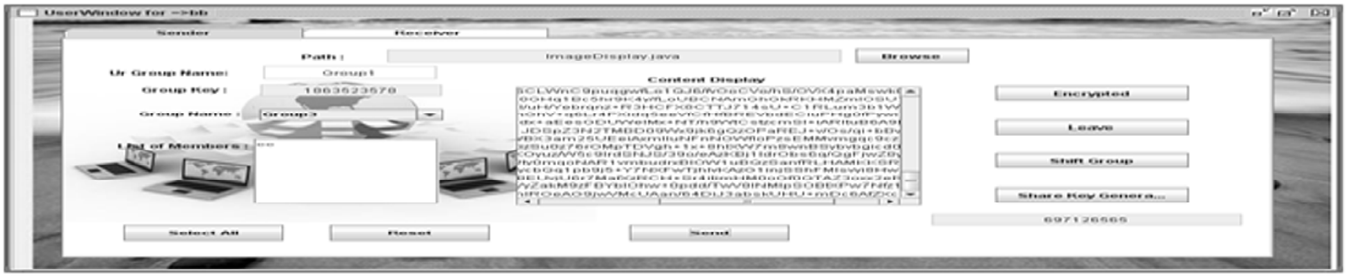
***Encryption data code:***

```
class Encrypted Data
{private static final String ALGORITHM = ″AES″;
private static final int ITERATIONS =2;
private static final byte[] keyValue =new byte[] {″T″, ″h″, ″i″, ″s″, ″I″, ″s″, ″A″, ″S″, ″e″, ″c″, ″r″, ″e″, ″t″, ″K″, ″e″, ″y″};
public static String encrypt(String value, String salt) throws Exception{
Key key = generateKey();
Cipher c = Cipher.getInstance(ALGORITHM);
c.init(Cipher.ENCRYPT_MODE, key);
String valueToEnc = null;
String eValue = value;
for (int i = 0; i < ITERATIONS; i++){valueToEnc = salt + eValue;
byte[] encValue = c.doFinal(valueToEnc.getBytes());
eValue = new BASE64Encoder().encode(encValue);}
```

Discussion: This is the receivers side window where the data has been sent.

***Decrypt code:***

```
public static String decrypt(String value, String salt) throws Exception
{Key key = generateKey();
```



Path : ImageDisplay.java

Ur Group Name: Group1

Group Key : 1863523578

Group Name : Group3

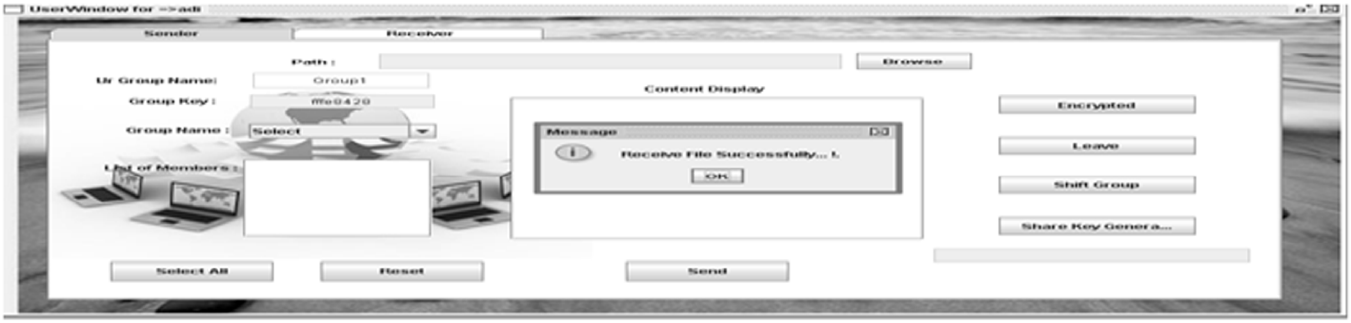
List of Members :

Content Display

[illegible]

697126565

**Figure 10: Encryption of Data**



Path :

Ur Group Name: Group1

Group Key : ffe0420

Group Name : Select

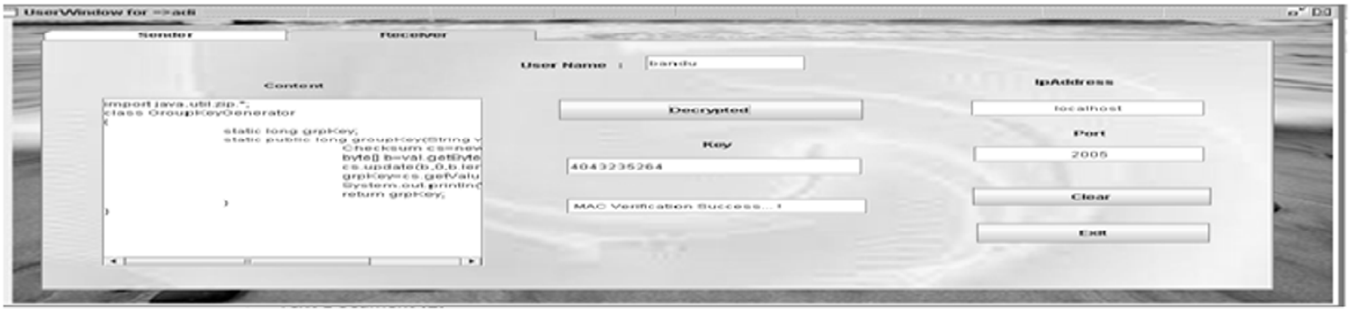
List of Members :

Content Display

Message

Receive File Successfully... !

**Figure 11: User Received Data**



User Name : bandu

Content

```
import java.util.zip.*;
class GroupKeyGenerator
{
                static long grpKey;
                static public long groupKey(String v
                                Checksum cs=new
                                byte[] b=val.getByte
                                cs.update(b,0,b.ler
                                grpKey=cs.getValu
                                System.out.println(
                                return grpKey;
                }
}
```

Key

4043235264

MAC Verification Success... !

IpAddress

localhost

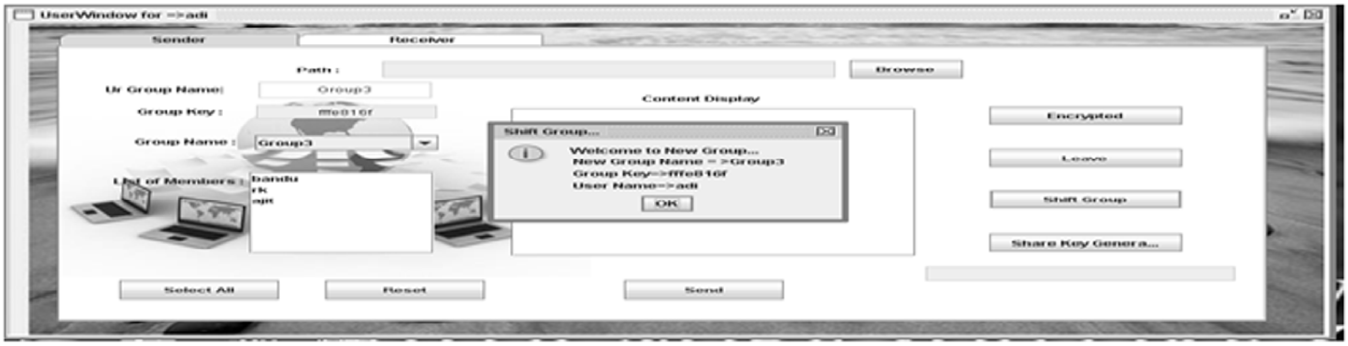
Port

2005

**Figure 12: Data in Decryption Form**

```
Cipher c = Cipher.getInstance(ALGORITHM);
c.init(Cipher.DECRYPT_MODE, key);
String dValue = null;
String valueToDecrypt = value;
for (int i = 0; i < ITERATIONS; i++){
byte[] decordedValue = new BASE64Decoder().decodeBuffer(valueToDecrypt);
byte[] decValue = c.doFinal(decordedValue);
dValue = new String(decValue).substring(salt.length());
valueToDecrypt = dValue;}return dValue;}
public static Key generateKey() throws Exception{
Key key = new SecretKeySpec(keyValue, ALGORITHM);
String k=key.toString();
String[] k1=k.split("@");
return key;}
```

Discussion: Server first match the share key if it will match then users can decrypt the data.



Ur Group Name: Group3

Group Key : fffe816f

Group Name : Group3

List of Members : bandu<br>rk<br>ajit

Welcome to New Group...
New Group Name = >Group3
Group Key=>fffe816f
User Name=>adi

**Figure 13: Shifting of Group**

Discussion: User can shift their group by using the button shift group. Then message box show users shifting information**.**

## 5. CONCLUSION AND FUNCTURE ENHANCEMENT

### 5.1. Conclusion

In this Paper, a user revocation scheme is proposed which can be well adopted into MSN. The proposed scheme enables a TA to efficiently revoke a specific user's decryption capability without any effect on other users' capability. By security analysis, we have verified that attribute collusion attacks and revoke collusion attacks can be prevented by the proposed scheme. Through extensive simulations, it has been demonstrated that although the proposed scheme requires a small increase of user-secret-key size, it outperforms the existing solution in terms of reduced amount of updated information and fast update process. Since the update percentage over time increases greatly if cooperative transmission is engaged among mobile social users for distributing the update information, for our future work, develop a cooperation incentivizing mechanism to encourage users to transmit the update information in a distributed manner.

## 5.2. Future Enhancement

Online Social Networks have become an important part of daily digital interactions for more than half a billion users around the world. The various personal information sharing practices that online social network providers promote have led to their success as innovative social interaction platforms In purposed system, it consider about only the communication between the same group members. In future, we discuss about communication between the different group members in that direction.

## REFERENCES

[1] Chen, L., Lu, R., Liang, X., Lin, X., and Shen, X.S., "*Journal of Communications and Networks*", vol. 13, no. 2, pp. 102–112, 2011.

[2] Attrapadung, N., and Imai, H., "Attribute-based encryption supporting direct/indirect revocation modes," 2009.

[3] A. Ronald Tony, D. Saravanan, Text Taxonomy using Data mining clustering system, Asian Journal of information technology, 14(3), 97-104, 2015.

[4] D. Saravanan, V.Somasundaram "Matrix Based Sequential Indexing Technique for Video Data Mining "Journal of Theoretical and Applied Information Technology 30th September 2014. Vol. 67, No. 3 pp. 725-731.

[5] Liang, X., Lu, R., Lin, X., and Shen, X., in *GLOBECOM*, "Message authentication with non-transferability for location privacy in mobile ad hoc networks," 2010.

[6] Pearson Prentice Hall, Fourth Edition Written by William Stallings Published by Dorling Kindersley (India) Pvt, Ltd., licensees of Pearson Education in South Asia. "Cryptography and Network Security".

[7] D. Saravanan, Effective Multimedia Content Retrieval, International Journal of Applied Environmental Sciences, Volume 10, Number 5 (2015), pp. 1771-17783.

[8] Dylan Andrew Harper Smith, Changcheng Huang, James Yan, "Hierarchical Notification Dissemination for IMS Presence Using Network Coordinates", In the proceeding of IEEE Global Telecommunication Conference, pp. 429-433. 2010.

[9] Y. Cifuentes, L. Beltrán, L. Ramírez, "Analysis of Security Vulnerabilities for Mobile Health Applications", World Academy of Science, Engineering and Technology International Journal of Electrical, Computer, Energetic, Electronic and Communication Engineering Vol. 9, No. 9, 2015, pp. 1016-1021.

[10] D. Saravanan, Performance Anlaysis of video data image using Clustering Technique, Indian journal of science and technology, Vol. 9 (10, March 2016, ISSN (Print) : 0974-6846.

[11] D. Saravanan (2015). Literature Survey on Web Based Knowledge Extraction, i-manager's Journal on Software Engineering, 10(2), Oct-Dec 2015, Print ISSN 0973-5151, E-ISSN 2230-7168, pp. 38-42

[12] Mangey Ram , Kuldeep Nagiya , "Performance evaluation of mobile communication system with reliability measures", International Journal of Quality & Reliability Management, Vol. 33 Iss: 3, pp. 430–440.