Prevention of Losing User Account by Enhancing Security Module: A Facebook Case

M. Milton Joe
Assistant Professor, Department of Computer Application,
St. Jerome's College, Nagercoil, Tamilnadu, India.
m.miltonjoe@gmail.com

Dr. B. Ramakrishnan,
Associate Professor, Department of Computer Science and Research Centre,
S.T. Hindu College, Nagercoil, Tamilnadu, India.
ramsthc@gmail.com

Dr. R.S. Shaji
Professor, Department of IT, Noorul Islam University, Nagercoil, Tamilnadu, India.
shajiswaram@yahoo.com

***Abstract*— The blooming development of internet technologies, lead to the growth of Online Social Networks (OSNs) day by day. There are many Online Social Networks (OSNs) came on internet but still very few could get the attraction of the users forever. The most attracted and world level leading Online Social Networks (OSNs) is Facebook, Twitter, and Google Plus and so on. All these Online Social Networks (OSNs) allow its users to create profiles and share any information on their profile, which could be viewed by other users of the same network user. These Social Networks allow users to form friendship with other people and make them to get connected in an easiest way. The major advantages of these Online Social Networks (OSNs) are getting connected with friends (wherever they are in the world), thoughts and ideas can be shared on online and feedback could be obtained as soon as possible. Every user of Social Networking sites will have many more confidential and private data on their account. However the Security and Quality of Service (QoS) are the major constraints must be always maintained in all the social networks. Most of the Online Social Networks (OSNs) provides security to the data available on the user account and provides good Quality of Service (Qos). Obviously the security constraint must be maintained not only the data available on user account but also must be maintained to the user account completely, which ultimately improves the efficiency of Quality of Service (Qos). In this paper, we evaluate and propose a new model to enhance the security for improving quality of service in online social networks.**

***Index Terms*— Online Social Networks (ONSs), Security, Quality of Service (QoS), Authentication, Random Number.**

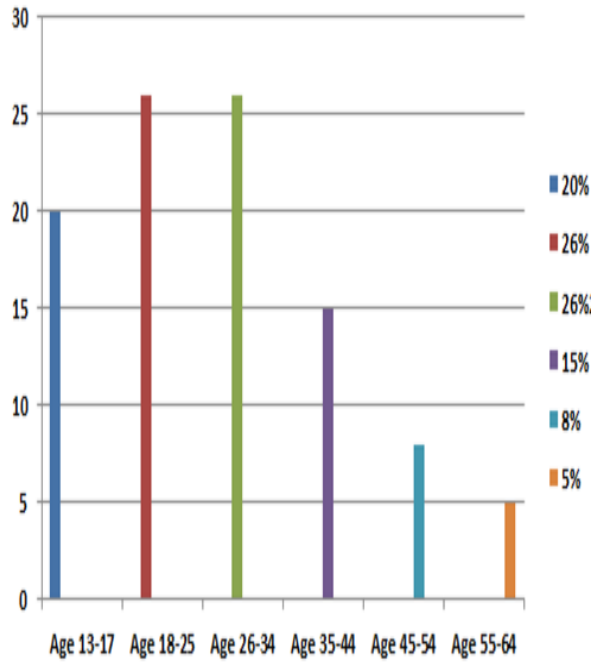
I. INTRODUCTION

The most common and easiest way to connect with friends, relatives and with other people is internet. The development of internet gradually made people to get connected and share ideas with one another in the form of establishing a network communication. The web 2.0 technology developments made this form of communication in the name of Online Social Networks (OSNs) [1], which made people to create profiles and share information available on their pro file to other users. There are many Online Social Networks (OSNs) do exist such as Facebook, Twitter, MySpace, and Google Plus but very few could stand among internet users and became popular. The active users of these Online Social Networks (OSNs) especially Facebook, and twitter almost crossed more than one billion [2] [3]. Among all the social networking websites, Facebook attracted many users in and around the world. Facebook needs a registration to open an account; the registration could be done with an E-mail id. Facebook was founded February 2004 and operated by Facebook community [4]. Facebook crossed over one billion active users during the month of September 2012, and more than half of whom use on mobile devices [4]. Facebook was founded by Mark Zuckerberg with his college roommates and fellow Harvard University students Eduardo Saverin, Andrew McCollum, Dustin Moskovitz and Chris Hughes [4]. Users of Facebook can create personal profile and add others as their friends by giving friend request and the other user must accept the friend request to become friend with them. The user of Facebook can share information and send message to the other user's message box or simple post the information on the wall of the user. The active user of Facebook can chat with the other active user but both of them must be friends on

doi:10.4304/jetwi.5.3.247-256

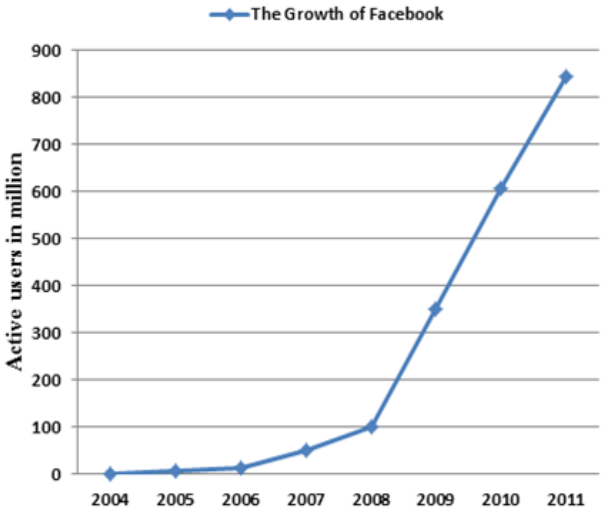
Facebook. Even though the user goes offline simply offline message can be sent to the user.

A January 2009 Compete.com study ranked Facebook as the most used social networking service by worldwide monthly active users[4]. Every day many new users are opening account on Facebook to get connected with their friends. The growth of Facebook also eventually increased day by day. The major reason for the growth of Facebook is, because it is very easy to use and it allows its user to post pictures and videos on their profile in a simplified way, which attracts most of the users. Users can comment on a picture as well as on any post made by the user in simplified manner, which could be viewed and notified to the others users immediately and reply back to the comment at once. According to a May 2011 *Consumer Reports* survey, there are 7.5 million children under 13 with accounts and 5 million under 10, violating the site's terms of service [4]. The Facebook site was mostly covered with the children and youngster of the all-around world.



Graph 1 Facebook users by age in percentage

The above graph 1 indicates the users of Facebook by age, the graph shows most of the users of Facebook come under the age 18 to 34. Facebook allows its users to set their own privacy policy, which enables the users to set whom should view the specific information of their profile and the information shared by them. Facebook has various useful privacy settings to prevent the private information of a particular user account. For instance, in Facebook we can set who could view our friends, whereas in all the other social networking websites the friend list is public. Also Facebook allows its users to go offline from chatting for a particular user, on other hand the user will be shown as available to other users except the particular user for whom it was set as offline from chatting. Such a fabulous facility made Facebook popular in a short period of time.



Graph 2 The growth of Facebook

Graph 2 shows the growth and popularity of Facebook by year wise from the year 2004 to 2011 [4]. As the graph represents Facebook achieved a big victory within a short period of time. As stated above even though Facebook became very popular among internet users, still it has certain limitations. Facebook provides full privacy policy to the information available on the user account alone. All the data available on a user account on Facebook is highly securable but it fails to provide the same security to the entire user account. However this limitation should be avoided to increase the usability and provide good Quality of Service (QoS) to all its users. In this paper, we provide an alternative method instead of the present method in order to provide security on user account and improve the Quality of Service (QoS).

II. Related Work

The users, who are aware of security, are able to set privacy policy to their profile object [5]. That is, users can divide their total number of friends into various groups such as schoolmates, college mates, family members and user can set privacy options to each group depending upon the priority. This type of different privacy setting to each group restricts one group members from viewing the personal photo of the user, while other group member can view the photo [5]. For grouping of friends effectively previous research was carried out based on clustering technology, which aid users in grouping their friends more efficiently [5]. When the growth of online social networking came into effect the third party applications started to access the information from the user profile of the online social networking websites. The third party applications also posted some sort of information about their applications on user profile. So ultimately the access control on user profile by the third party application must be securable [1].The earlier research had focused on mainly user-

to-user interactions in social networks, and seems to ignore the third party applications [1]. To control the third party application an access control framework is presented [1]. The framework is based on enabling the user to specify the data attributes to be shared with the application and at the same time be able to specify the degree of specificity of the shared attributes [1]. This mechanism controlled the third party application from preventing the private information of the user profile. Other related work has analyzed both privacy risks associated with information disclosure in social networks, and developed initial mechanisms to protect against some involuntary information disclosure and proposed a framework for deriving a "privacy score" to inform the user of the potential risks to their privacy created by their activities and activities with other users within the social network [7].However the previous research areas concentrated on friends grouping policy to enable different privacy setting to provide, which data should be accessed by which group of users and similarly work carried out to prevent the third party application from accessing the user data from the profile. A new framework was developed to give more security to the data available on user profile. All these privacy and security mechanisms provide protection only to the profile data of the user not to the entire user account. However every user account must be secured in all the ways from fraudulent access. We propose a new method to prevent the user account from being lost access by the owner of the corresponding user.

III. Problem Statement

The most popular Online Social Networks (ONSs) Facebook allow internet users to create personal profile and post photos, videos, share information and send message to friends. However this famous Online Social Network website has a security mechanism, which most of the times makes the corresponding author or the owner of the account to lose the access to the account. Let us consider the following scenario:

(1) Usually a user uses his/her mobile phone to login to Facebook. We know already more than half of Facebook users use mobile device to access Facebook [4]. However the user access Facebook on his/her mobile device for long days regularly and one day wishes to change the mobile device, which has more facility to get the access easier. When the device is changed and user tries to login in with the new device the Facebook application will prompt as follows:

(2) On the other hand if a user does not access his/her account for few months and tries to access his/her account with a new device; or unauthorized access is found; Facebook will prompt as follows:

- Your account is temporarily locked.
- Someone recently tried to log into your account from unrecognized device or location. Please verify if it was you who tried to log in.

The same case is also applicable when the user changes the laptop or desktop too. This type of security mechanism has major drawback, which is evaluated below.

A. Limitations of Existing Model

Once the account of a user is locked, it prompts the user to authenticate the user originality in the following ways.

- Provide your birthday.
- Identify the photos of friends.

Or try logging into Facebook from a device you have logged in before.

Case 1 - Provide your birthday: In every online social networking websites, the users may not wish to provide their real birthday especially VIP members like Politicians, actors, actress and others too. In this scenario they may give some dummy birthday details when they create the account on Facebook and they may not remember that birthday forever. When the access to the account is lost due to change of device and asking them to prove user originality by providing birthday is really a risk to the users.

Case 2 - Identify the photos of friends: As we all know, everyday many users will post more photos on Facebook and the user may not remember which photo was posted by which user. Let us assume a user does not log into his/her account for one month. So the user will not know whoever has posted photos and which photo posted during that one month. Identifying the photos of friend's means, a photo will be displayed and the user has to choose the correct friend (user) who had posted that photo among the list of friends shown. However the displayed photo will also be from the days while the user did not log into his/her account. So identifying the friends by random photos will be tougher and really risk to the users.

Case 3 - Device used before: The final way to logging into Facebook from a device you have logged in before. In this scenario, if the user has sold his mobile device to someone else or had lost his/her mobile device then how the user could could log in with the device used before. It also will be highly a risk to the users.

As presented above, all the present mechanism provided by Facebook to prove the originality of the user has a major drawback, risk and makes the original user to lose his/her account permanently. If the user has lost his account permanently, he/she will lose entire friend circle and all the information associated with account. However a new mechanism is needed, which enhance the security for improving the quality of service.

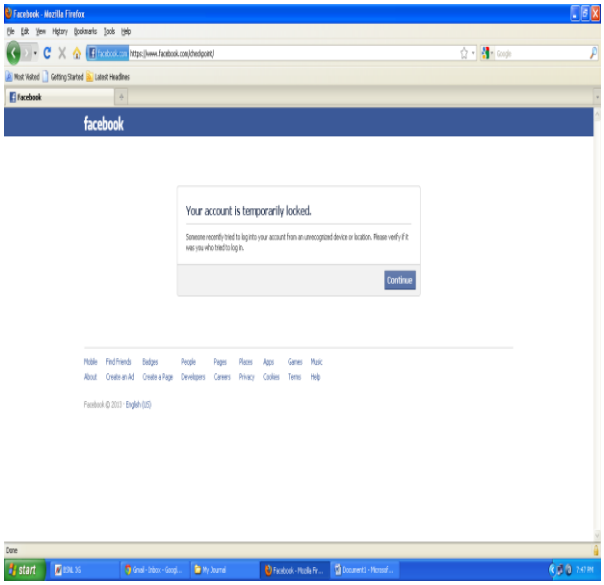


Fig 1 Account Temporarily Locked.

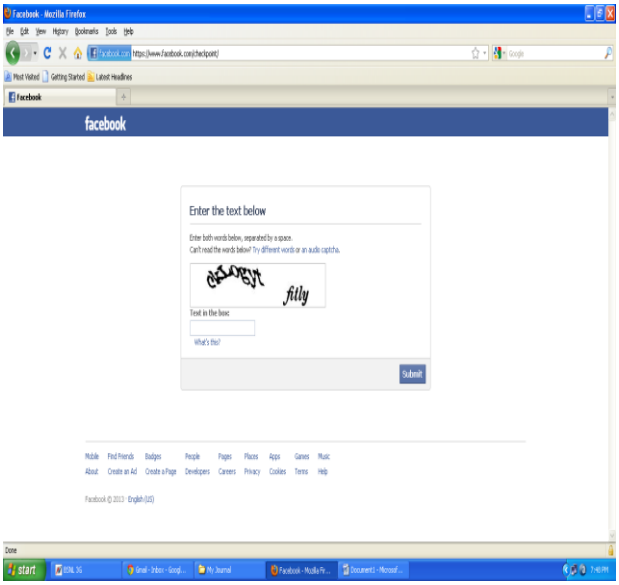


Fig 2 Enter the Text Below

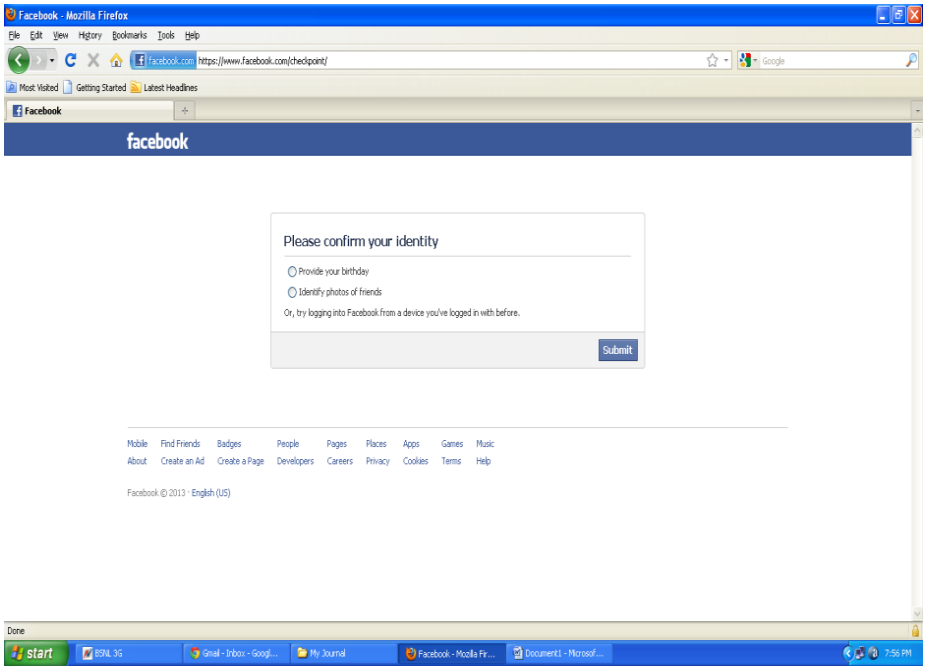


Fig 3 Confirm your identity

The above showm diagrams Fig 1, Fig 2, and Fig 3 represents the concept of Facebook to prove the originality of the user when the account is temporarily locked. However all these mechanism are not efficient and convenient for the internet users at all times. A new mechanism is ultimately needed to enhance the security for improving the quality of services in Online Social Networks (OSNs). The new system that we propose in this paper will always improve the efficiency and will be very much convenient to the internet users and also the proposed system will maintain the security constraints along with improved quality of service always.

B. Data Flow in Existing Model:

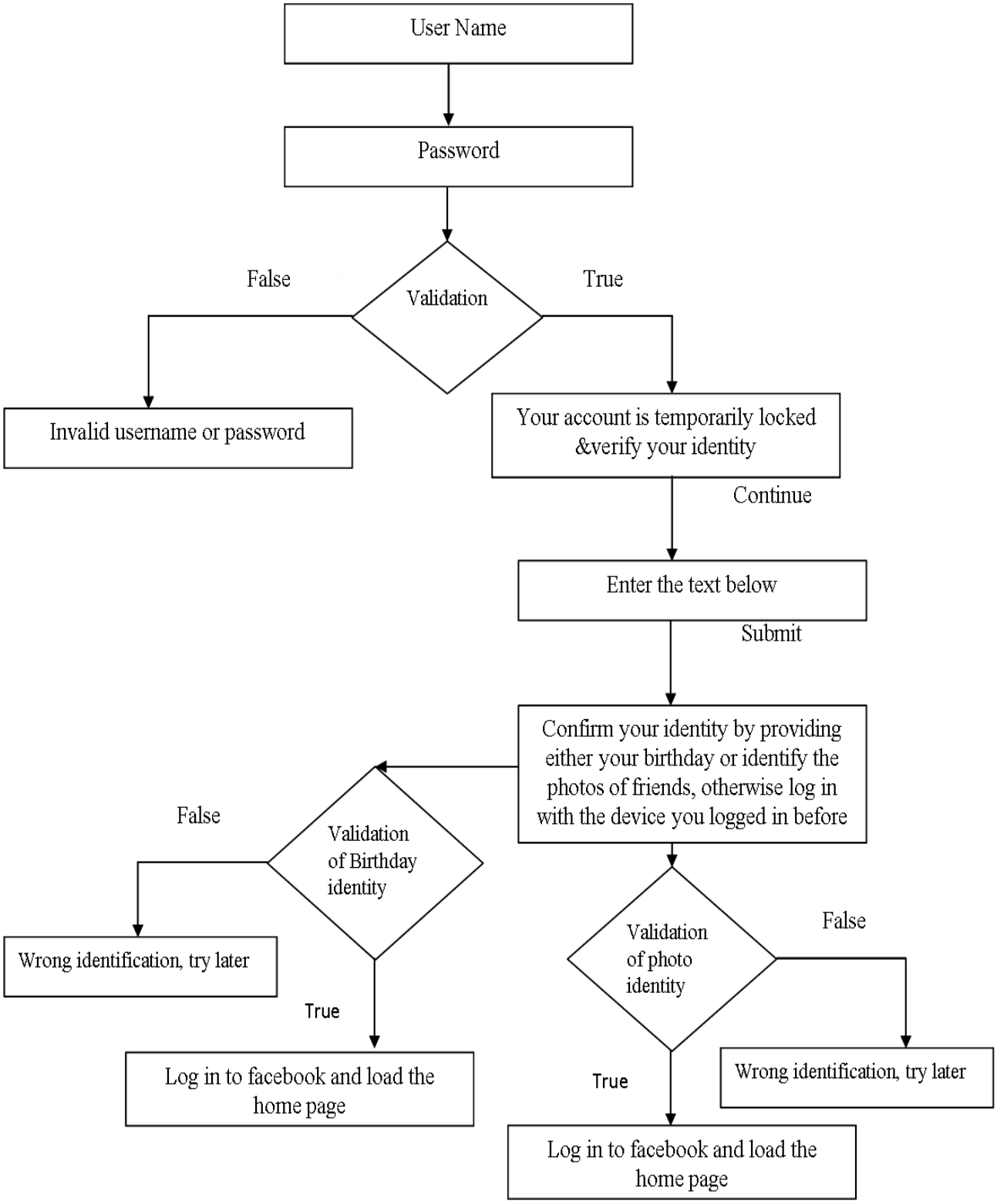


Fig 4 Data Flow in Existing Model

IV. Proposed Model

A. *Data Flow in Proposed Model:*

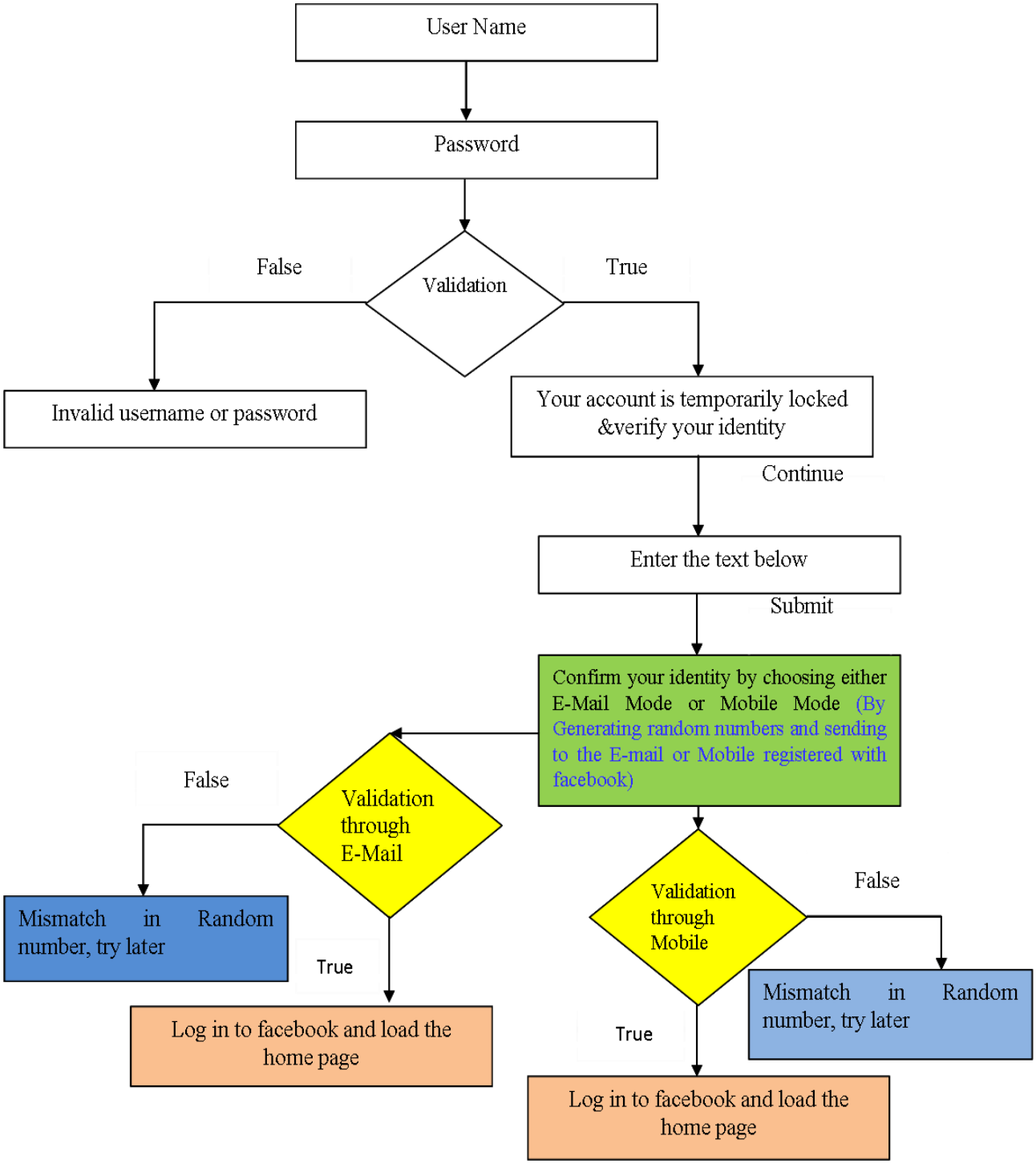


Fig 5 Data Flow in Proposed Model

The improvement of Quality of Service (QoS) by enhancing security mechanism in the proposed scheme can be evaluated as follows: when the user encounters the problem, while log in to his/her account such as the account is temporarily locked as shown below:

- Your account is temporarily locked.
- Someone recently tried to log into your account from unrecognized device or location. Please verify if it was you who tried to log in.

The current verification mechanism leads to poor performance and so in the proposed scheme we evaluate a new verification methodology, which maintains security constraint and improves quality of service always. The proposed verification scheme is shown and illustrated below.

- Validation through Mobile.
- Validation through E- Mail.

Case 1 – Validation through Mobile: In the proposed model, we propose the Facebook community organization should make its users give their mobile number compulsorily, while registering for new account creation. However the already existing users also must be asked to give their mobile number before logging into their account. If a user wishes to change his/her mobile number later that also must be allowed at any time. Later, whenever the account of any user is locked temporarily and the user chooses the validation through mobile, randomly generated number will be forwarded to the user's mobile number, which is associated with the corresponding user account. Once the user receives the randomly generated number on mobile must give the same number as input in the form, where the number is asked for validation. If both the numbers are same, the account is verified successfully and the user can have access to his/her account.

Case 2 – Validation through E- Mail: Account can be created in Facebook with an existing E- Mail id. However when the user account is locked temporarily and user chooses the validation through E- Mail, randomly generated number will be forwarded to the user's E- Mail id, which is associated with the corresponding user account. Once the user receives the randomly generated number on E- Mail must give the same number as input in the form, where the number is asked for validation. If both the numbers are same, the account is verified successfully and the user can have access to his/her account.

The above described to validation process methods replaces the existing methods available presently. Our proposed scheme uses random generated numbers to validate the user account and prove the user originality. This new scheme will enhance the security of the user account and also it improves the quality of service to Facebook users always. The implementation of our proposed scheme will make Facebook users not to lose access to their accounts and they will get connected with their friends, families and so on.

V. Implementation

The implementation of the proposed scheme can be carried out by generating random numbers. A random number is a number generated by a process, whose outcome is unpredictable, and which cannot be sub sequentially reliably reproduced [8]. The generation of random numbers cannot be guessed by previous value. This random number generation is used in most of the applications especially web applications. Here, in the proposed model we generate random numbers using the programming language JAVA. Java language is fully object oriented and highly securable language. Java language supports for generating random numbers by its packages. The Random class must be imported to generate random number in Java programming language as shown below.

- import java.util.Random;

Next the random object must be created to generate the random numbers. This random object allows the programmer to generate the simple random number generator. The predefined methods associated with the random object will generate the random numbers within the range of values.

(1) Random rand = new Random (); } Random object creation

(2) nextInt() & nextLong() } Methods of Random object

Let's consider the following Java programming that generates the random number, which cannot be predicted by the user.

```
import java.util.Random;
{
class number
{
   public static void main(String args[])
   {
  Random rand= new Random();
       for(j=0;j<1;j++)
       {
           System.out.println(rand.nextInt());
           System.out.println();
       }
   }
}
```

The above program will produce the random numbers as shown below, for each execution different number will be generated as shown below.

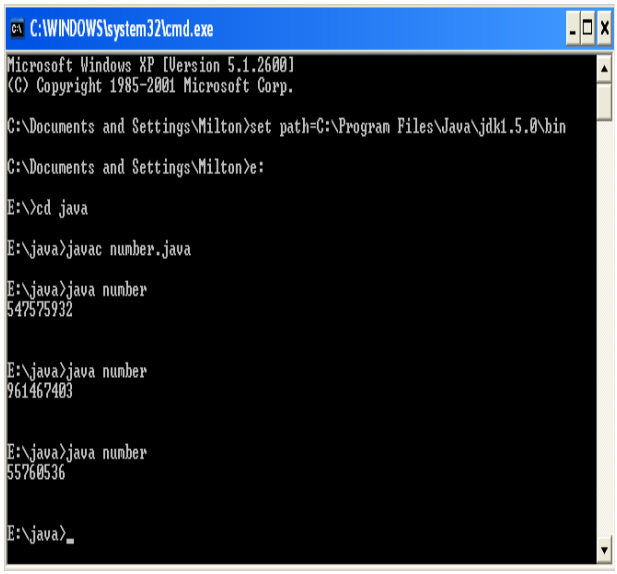


Fig 6 Random Numbers

The fig 6 shows the three different values generated by the same programming code for its three executions. However the same program can be executed as many times as need for the random numbers. The execution of for loop can be maximized if it is needed for the application. This random number can be used in our proposed model to enhance the security and also to improve the quality of service in online social networking.

In the proposed model, when the user account is temporarily locked the user must gone through the validation process to prove the use originality. The validation process can be done in the following two ways.

- Validation through Mobile.
- Validation through E- Mail.

If the user chooses the validation through mobile, the generated random number can be sent to the user's mobile device that is registered with the Facebook account and the received verification code is asked to be given in the form of Facebook application to validate the user. The user will be validated if the entered data on the form matches with the generated random number.

If the user chooses the validation through E- Mail, the generated random number can be sent to the user's E- Mail that is registered with the Facebook account and the received verification code is asked to be given in the form of Facebook application to validate the user. The user will be validated if the entered data on the form matches with the generated random number. Thus the proposed model uses random number generation methods to prove the user originality forever. This validation process is simple and will be very much convenient to the Facebook users. The implementation of the proposed scheme will make the Facebook users get connected with their friends and prevent them from losing access to their account.

VI. Results

The following screenshots represent the execution of our proposed data flow model, which enhance the security for improving the quality of service in online social networks.

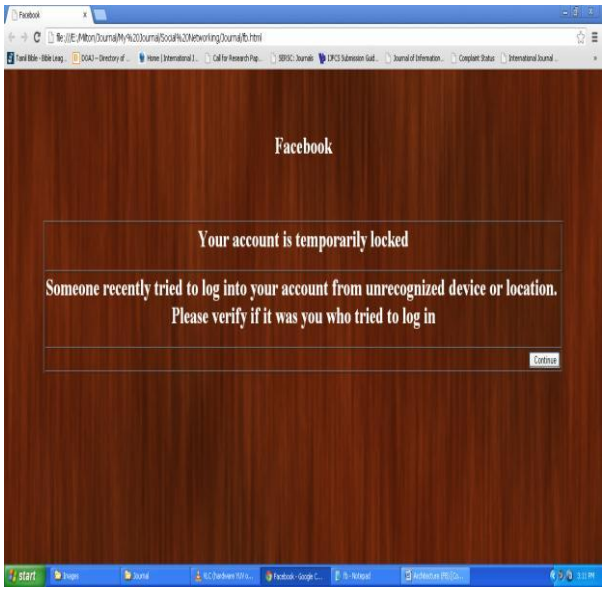


Fig 7 Account Temporarily Locked.

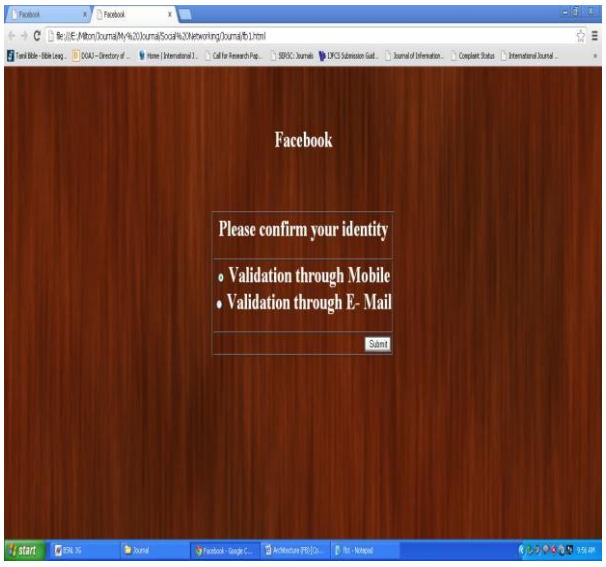


Fig 8 Validation Process

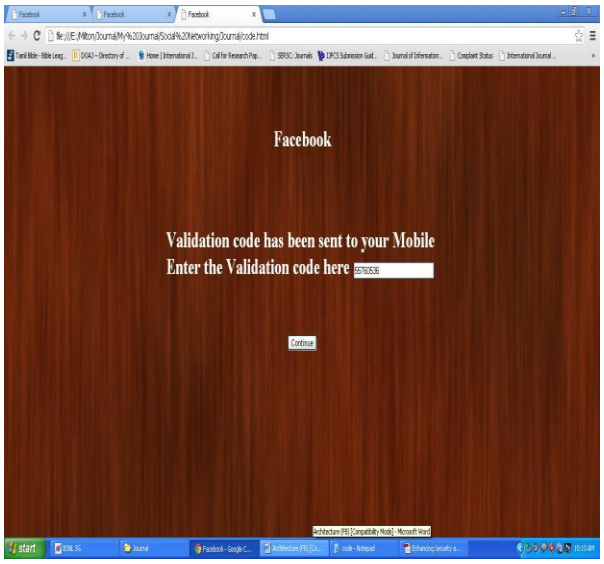


Fig 9 Validation through Mobile

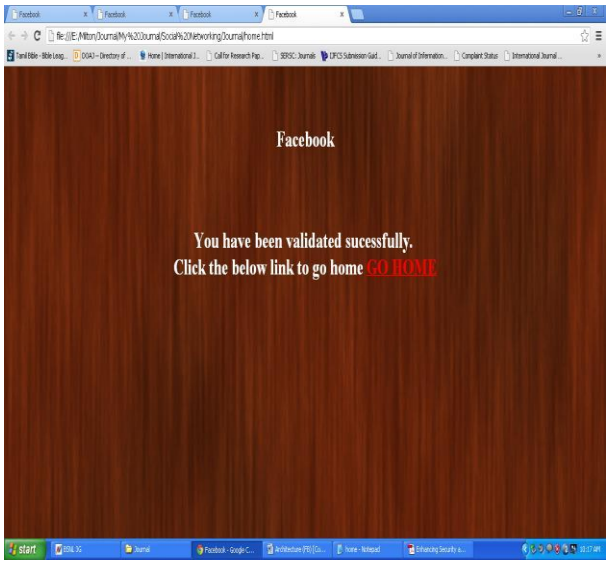


Fig 10 User validated successfully

The fig 7 shows the user account temporarily locked, when the user changes his/her device after long period of time being used the same device. The user account will be also temporarily locked, if some unauthorized user tries to access another user's account. Fig 8 represents the proposed data model concept of validating a user, after his/her account is temporarily locked. The proposed validation process can be carried out by either validation through Mobile or validation through E- Mail. The fig 9 shows the validation process of a user to prove the user originality through mobile. When the user chooses the validation process through mobile, automatically generated random number will be sent to the user's mobile device that is registered with the Facebook account. Once the random number is sent to the user's mobile device the user will be asked to give the validation code as input in the form as shown in the fig 9. After entering the validation code in the form, the entered code is matched with the generated code for the particular user. If both codes are matched, the user is validated successfully and the temporary lock is released and the user is allowed to go to his homepage as shown in the fig 10. If mismatch is found between codes, the user is not validated successfully and the user will not be allowed to go his/her homepage. The same process is applied, when the user chooses the validation process through E- Mail. Once the user have chosen the validation process through E- Mail, the automatically generated random number is sent to the user's E- Mail id that is registered with Facebook account and the user will be asked to enter the validation code in the Facebook form to check the user originality. If both codes are matched, the user is validated successfully and the temporary lock is released and the user is allowed to go to his homepage as shown in the fig 10. If mismatch is found between codes, the user is not validated successfully and the user will not be allowed to go his/her homepage.

CONCLUSION

In this paper, we have studied the comprehensive characteristics of Facebook application and we found Facebook application is lacking to produce security constraint to entire user account by its existing data flow model, which degrades the quality of service in Facebook application. We have proposed a new data flow model for Facebook application, which ultimately enhance the security constraints for improving the quality of service in facbook application. Our proposed model is evaluated and expected outcome is obtained at security level and improving quality of service.

REFERENCES

[1] Mohamed Shehab a, Anna Squicciarini b, Gail-Joon Ahn c, Irini Kokkinou "Access control for online social networks third party applications" Elsevier- Computers & Security 31 (2012) 897-911.
[2] Facebook, Facebook Statistics, March 2011. <http://www.Facebook.com/press>.
[3] Twitter, Twitter Numbers, March 2011. <http://blog.twitter.com/2011/03/numbers.html>.
[4] Facebook, http://en.wikipedia.org/wiki/Facebook
[5] Gorrell P. Cheek, Mohamed Shehab "Policy-by-Example for Online Social Networks" SACMATO 12 JUNE 20-22, 2012 NEWARK, NEW JERSY, USA, ACM YEAR 2012.
[6] Liu Kun, Terzi Evimaria. A framework for computing the privacy scores of users in online social networks. In: ICDM 2009, the ninth IEEE international conference on data mining, pp.288e297; December 2009.
[7] H. Kim, J. Tang, R. Anderson, Social authentication: harder than it looks, in: Proceedings of the 2012 Cryptography and Data Security Conference, 2012.
[8] M. Gjoka, M. Kurant, C.T. Butts, A. Markopoulou, Walking in Facebook: a case study of unbiased sampling of osns, in: Proceedings of IEEE INFOCOM '10, San Diego, CA, 2010.
[9] A.S. Yuksel, M. E. Yuksel, and A. H. Zaim. An approach for protecting privacy on social networks. In Proceedings of 5th International Conference on

Systems and Networks Communications, Washington, DC, USA, 2010. IEEE Computer Society.

[10] A.Acquisti and J. Grossklags. Privacy and rationality in individual decision making. IEEE Security and Privacy, 3(1):26{33}, 2005.

AUTHORS

Mr. M. Milton Joe was born in Nagercoil, Tamilnadu, India in 1988. He received his B.Sc Computer Science degree from Bharathidasan University, India in 2009 and he received his MCA degree from Anna University, India in 2012. Thereafter he worked as Assistant Professor in Meenakshi Academy of Higher Education and Research (Meenakshi University) for a year. Presently he is working as Assistant Professor at St. Jerome's College in Nagercoil, Tamilnadu, India. He has authored five research papers in reputed International Journals. His research topic includes Network Security, Network Communication, Vehicular Network and Social Networks.

Dr. B. Ramakrishnan is currently working as Associate Professor in the Department of Computer Science and research Centre in S.T. Hindu College, Nagercoil. He received his M.Sc degree from Madurai Kamaraj University, Madurai and received Mphil (Comp. Sc.) from Alagappa University Karikudi. He earned his Doctorate degree in the field of Computer Science from Manonmaniam Sundaranar University, Tirunelveli. He has a teaching experience of 26 years. His research interests lie in the field of Vehicular networks, mobile network and communication, Cloud computing, Green computing, Ad-hoc networks and Network security.

Dr. R.S. Shaji received his M.Tech in Computer Science and Engineering from Pondicherry University and PhD from Manonmaniam Sundaranar University. Presently he is working as Professor in Noorul Islam University. He has seven years of research experience and published more than twenty international journals. His research interests include Mobile and pervasive Networks.