

# **Prevention of Unauthorized Access in Social Networks Using Authentication**

**Progress Report**  
**In fulfillment of the requirements for the**  
**NU 302 R&D Project**  
**At NIIT University**



**Submitted by:**

Akshat Khanna(U101115FCS046)  
Divya Chadha(U101115FCS196)  
Sarthak Kohli(U101115FCS141)  
Sheldon Dsouza(U101115FCS144)  
Simran Senapati(U101115FCS231)

**Area**  
**NIIT University**  
**Neemrana, Rajasthan**

# **CERTIFICATE**

This is to certify that the present research work entitled "Prevention of Unauthorized Access in Social Network Using Authentication" being submitted to NIIT University, Neemrana, Rajasthan, in the fulfillment of the requirements for the course at NIIT University, Neemrana, embodies authentic and faithful record of original research carried out by *Akshat Khanna, Divya Chadha, Sarthak Kohli, Sheldon Dsouza & Simran Senapati* students of B Tech (CSE) at NIIT University, Neemrana,. She /He has worked under our supervision and that the matter embodied in this project work has not been submitted, in part or full, as a project report for any course of NIIT University, Neemrana or any other university.

Name and Title of the Mentor

**Prof. Manoj Kumar**

# **List of Figures**

Fig 1: Digital Image, Source: Google

Fig 2: Digital Image, Source: Google

Fig 3: Digital Image, Source: Google

Fig 4: Digital Image, Source: Google

Fig 5: Result 1, Source: Self

Fig 6: Result 2, Source: Self

Fig 7: Result 3, Source: Self

Fig 8: Result 4, Source: Self

Fig 9: Result 5, Source: Self

# CONTENTS

<b>Serial Number</b>	<b>TITLE</b>	<b>Page Number</b>
1.	Certificate	2
2.	List of Figures	3
3.	Rationale of Work	5
4.	Literature Review	6
5.	Objectives	13
6.	Methodology	14
7.	Results	19
8.	Summary	24
9.	Future Work	25
10.	References	26

# **Rationale of Work**

Online Social Network (OSN) is the most widely used platform to communicate with one another. It is fast and cheap when compared to other modes of communication. However, Online Social Network profiles are being hacked often by employing various types of malicious attacks. Most of the times the attackers are successful in accessing the OSN account which illustrates that the present authentication mechanisms are not efficient enough. Once an online social network account is being hacked, it can be misused widely and the hacker makes the authorized user unable to login to the account by changing the login credentials. Security in OSN must be provided and it must prevent the attacks aimed by the attackers. However, to prevent unauthorized access in OSN a novel authentication procedure is needed and the novel authentication mechanism must abide the social network platform characteristics.

The main motive for this project is to enhance the security of Online Social Network users by finding a novel authentication mechanism which must abide the social network platform characteristics.

# **Review of Literature**

## **Effectiveness of Social Media as a tool of communication and its potential for technology enabled connections: A micro-level study Trisha Dowerah Baruah (2012)**

One of the most important advantages of the use of social media is the online sharing of knowledge and information among the different groups of people. Today most of the people specially the youngsters are hooked on to the different social media for keeping in contact with their peers. It helps us to spread awareness. We can get connected to the world with just one click of a mouse. The main advantages of social media are:

- Sharing of ideas
- It is used as a tool for communication
- Bridges communication gap
- Is a source of information
- Important marketing tool
- Important customer interaction tool
- It is less time consuming
- Cost effective

Since we share our personal information on these rapidly growing internet platforms, its security is very important. If an online social network account is being hacked, it can be misused widely and the hacker makes the authorized user unable to login to the account by changing the login credentials. Security in OSN must be provided and it must prevent the attacks aimed by the attackers.

## **Access control for online social networks third party applications**

## **M Shehab, A Squicciarini, GJ Ahn, I Kokkinou (2012)**

The paper discusses about the threats that online social networks possess as we provide many of our personal information on such sites. And how it's access can be controlled. Online social networks are able to provide open platforms to enable the seamless sharing of profile data to enable public developers to interface and extend the social network services as applications. At the same time, these open interfaces pose serious privacy concerns as third party applications are usually given access to the user profiles. Current related research has focused on mainly user-to-user interactions in social networks, and seems to ignore the third party applications.

The recent growth of social network sites such as Facebook, Twitter and MySpace has created many interesting and challenging security and privacy problems. In social networks, users manage their profile, interact with other users, and self-organize into different communities. Users profiles usually include information such as the user's name, birthdate, address, contact information, emails, education, interests, photos, music, videos, blogs and many other attributes. Controlling access to the information posted on user profile is a challenging task as it requires average Internet users to act as system administrators to specify and configure access control policies for their profiles. To control interactions between users, the user's world is divided into a trusted and a non-trusted set of users, typically referred to as *friends* and *strangers* respectively.

Users are provided with group based access control mechanisms (Facebook Inc, 2011) that apply access rules on the different groups of friends and strangers. Facebook, one of the most popular social sites, enables users to create friend lists and to compose profile policies based on these friend lists (Facebook Inc, 2010). Social networks platforms have focused on user-to-user fine grain access control; for example, the Facebook Privacy Policy allows users to specify fine grain policies controlling which profile attributes can be accessed by their friends and friends of friends (Facebook Inc, 2009).

## **Novel authentication procedures for preventing unauthorized access in social networks (2016)**

Looking at the matter of security over OSN platforms, **M. Milton Joe<sup>1</sup> & B. Ramakrishnan** published a paper in 2016 stating two modules that may help in securing OSN platform from unauthorized access. The two modules proposed by them were, CHAT MODULE and Relationship authentication module.

1. Chat module statistics.

Every social media user has a chat box which is private. The proposed module would increase a counter value whenever, the user chats with someone (sends and receives message). A cluster of frequently chatted users is created based upon the frequency and other grouping algorithms. This counter value will be helpful for authenticating the user when temporary locked out of OSN platform like Facebook due to suspicious attempt to login. The user would be asked to choose the most frequently chatted person among the 8 options provided in the question to prove his/her authentication.

2. Relationship circle module

On social media platforms like Facebook users classify their friends into categories like relationships (cousin, brother, sister, etc.) and types of friends (schoolmate, colleague, etc.). According to this module, the originality of users will be proved by relationship circle of the particular user profile. Among the various relationship circles of the user, he/she will be questioned about any one and the user needs to answer exactly according to the question asked.

A clear representation is given in the picture.

However, these modules have some loopholes or special cases where they will fail to check authenticity. If the person who wants to access a user's account is the frequently chatted person itself, he/she may easily answer the question and get access. The attacker may use a chat bot to increase the counter value and then use it accordingly. Similar case is there with the relationship module- If the attacker is someone who has quite a good knowledge about user's relationship circles can easily crack through these modules.

### **Security Issues Challenging Facebook**

**By: S Leitch, M Warren (2009)**

This paper states about the security issues faced by Facebook Verifying the identity of a Facebook user could be an issue. Identity theft is possible if social



engineering techniques or by the use of key logging software. There is Difficulty in verifying identify due to limited Facebook authentication, e.g. user name and password and Facebook request a mobile phone number in certain circumstance, e.g. being able to quickly reply to messages. Facebook users may accidentally alter their privacy settings and unintentionally release their information.

## **A Secure Simple Authenticated Key Exchange Algorithm based Authentication for Social Network**

**P Venkateswari, T Purusothaman - 2011**

Through this paper we come across different way of attacks that attackers practice to play with password and PIN-based user authentication. Many security systems are designed in such a way so that security relies entirely on a secret password. There are password cracker programs, like key logging, random guessing etc., due to which users need to create unpredictable passwords, which are more difficult to remember. They eventually end up writing them down somewhere which is quite vulnerable. The pure character based password is less secure, since it is easily breakable either by Brute force attack or through Dictionary attack. Mostly it is a combination of alphabet and numerals. Passwords can be revealed by trying through various possibilities in brute force attack. In dictionary attack, crackers can try with any meaningful words of a dictionary.

Password based authenticated key has recently received attention in this field as in general the classical password schemes are prone to the attacks discussed earlier. Most of the network security protocols provide security based on cryptography techniques. The keys should be generated secretly and distributed. The study discuss on three related components that were considered for the proposed security measures, namely shared keys based on passwords security methods, personalized questions and one time passwords. The study elaborated shared key for authentication. Shared key methods have proved to be effective in withstanding general attacks.

This approach gave us a direction for what we came up with.

**Personal knowledge questions for fallback authentication:  
Security questions in the era of Facebook**

## **A Rabkin (2008)**

Security questions (or challenge questions) are commonly used to authenticate users who have lost their passwords. They performed a survey on banking users to discuss patterns in the security questions. We argue that today's personal security questions owe their strength to the hardness of an information-retrieval problem. However, as personal information becomes ubiquitously available online, the hardness of this problem, and security provided by such questions, will likely diminish over time. Six possible weaknesses in this method were observed: inapplicability, ambiguity, and lack of memorability, guess ability, attack ability, and automatic attack ability.

### **Inapplicability:**

Some security questions are simply inapplicable to a large fraction of the public. For instance, "Which high school did your spouse attend?" is inapplicable to unmarried individuals.

### **Ambiguity:**

If the questions have changing answers then it becomes difficult to remember the answer that user provided while creating the profile, and thus can get confused between the earlier answer and the present answer. For eg: Your favorite music.

### **Lack of memory**

Some question like what was the last name of your kindergarten teacher? Or where did your mother was born are difficult to recall. The secret questions are answered during the creation of profile / registration of profile, thus it becomes difficult for user to remember them as they are used very less times.

### **Guess ability**

The questions which may have general answer or predictable answer comes under this category (age related questions, passing year of school, etc.)

### **Attackable**

An attacker who may know victim's identity and knows the answer to the questions provided can easily prove user's authentication and then misuse the profile data. The questions like What is your pet's name were classified in this category.

### **Automatically attackable**

A question is classified as automatically attackable if it had an answer that would be visible in the structured portion of a user's profile page on Facebook or similar social net-working websites. Date of birth and ZIP code, which are often mandatory questions, fall into this category. Here some of the facebook data or other algorithms can be used to automatically generate/ guess the answers

By reading this paper, we can conclude that the existing authentication method/module of authentication i.e. security questions and answers have their own deficiency and are not very reliable.

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

**MM Joe, B Ramakrishnan, RS Shaji (2013)**

This paper provides a summary/ study of the existing authentication methods in Facebook. 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 or makes anyone else easily use it. The mechanisms work after your profile is temporarily locked.

A Facebook profile gets temporarily locked when a user makes several attempts to login with a wrong password. 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 log in with the device used before. It also will be highly a risk to the users.

There is another authentication system of Facebook that uses email or mobile verification. In this mechanism, when unauthorized access is suspected, the user gets temporarily locked and then can choose between either Mobile or E-mail as the authentication parameter. A randomly generated number is sent to the selected option and user has to enter that pin. This method is not so secure yet as third parties are included and only one layer of security is there.

# **Objectives**

The main Objective of this project is to enhance the security of Online Social Network users by finding a novel authentication mechanism which must abide the social network platform characteristics.

# Methodology

## What we have surveyed

- The proposed procedures listed in the literature we surveyed make use of the user chatting module statistics. A counter variable is incremented whenever a conversation occurs between a sender and a receiver.

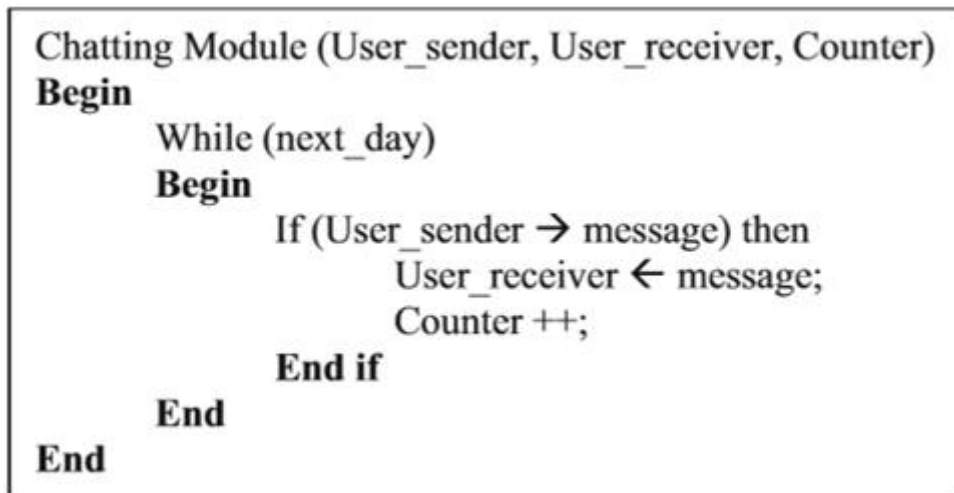


Fig 1

- The other one uses Relationship Circles authentication**, here the originality of users will be proved by relationship circle of the particular user profile like grouping of friends is done and a desired name is assigned to the groups.

```

Relationship_Circle (User)
Begin
  Name [n];
  Int i;
  Get the user profile that needs to be authenticated;
For (i=0; i<n; i++)
  Begin
    Circle = math * random (all relationship circle) //selects one relationship circle
  End for
For (i=0; i<n; i++)
  Begin
    Name[n] = math * random (circle) //selects one name from the selected circle
  End for
For (i=0; i<n; i++)
  Begin
    If (all the circles  $\neq$  circle) Then
    Do
      Name[n] = math * random (all the circles) //selects list of other names
    End if
  End for
  Print "who is your schoolmate?"
For (i=0; i<n; i++)
  Begin
    Print list of names in random order - Name [n];
  End for
End

```

**Fig 2**

But, there were some drawbacks with these methods like in the first method there might be a case where attacker could be a frequently chatted person himself or the attacker could use an AI chat bot that will contact the victim through the chatting mechanism. In the other method, there might be a case where the attackers knows about your circle.

The above proposed methods were implemented, and there authentication was proved to be not that much secured as already discussed in the drawbacks. *Password based authentication* can be easily cracked through keylogger, brute force attack, dictionary attack. Whereas in *Privacy based Question authentication*, there might be a case where the user has forgotten the answer of the question or it

is easily guessable by closed ones. In the case of *2-Factor Authentication*, a physical token is required and a memorized code which again one can forget that over the years. So these are some methods which are fine but the security is compromised.

## Experiment and Result

We did a lot of research in the area of authentication and much more experimentation. Analyzing the model and then proposing our very own model or experiment. So, then we came up with a **Picture Password**.



**Fig 3**

Picture Password, is a feature that allows you to create three different gestures on any image of user's choice and use those gestures as your password to login back. The gesture can be any combination of circles, straight lines and taps. There was a drawback in this experiment we performed, such password aren't inherently better than your old alphanumeric passwords, but they could be a more convenient (and no less secure) way to log in to your account. Also, these gestures adds as an alternative to the already defined authentication but they are not much secured as seen later. The other drawbacks we observed were, this is already an existing Microsoft feature and will create copyrights issue later if implemented. Therefore, we came up with another experiment as mentioned below:



## Our Final Work

As it has been seen that there are many algorithms for security purposes, one of which is RSA. And we came up with this idea of implementing RSA in our project.

- **RSA** which is named after its three developers Ron **Rivest**, Adi **Shamir**, and Leonard **Adleman**.
- It is a cryptosystem for public-key encryption, and is widely used for securing sensitive data, particularly when being sent over an insecure network such as the internet.
- It is an asymmetric cryptography algorithm which means that it works on two different keys, i.e., **Public Key** and **Private Key**.
- RSA keys can be typically 1024 or 2048 bits long.

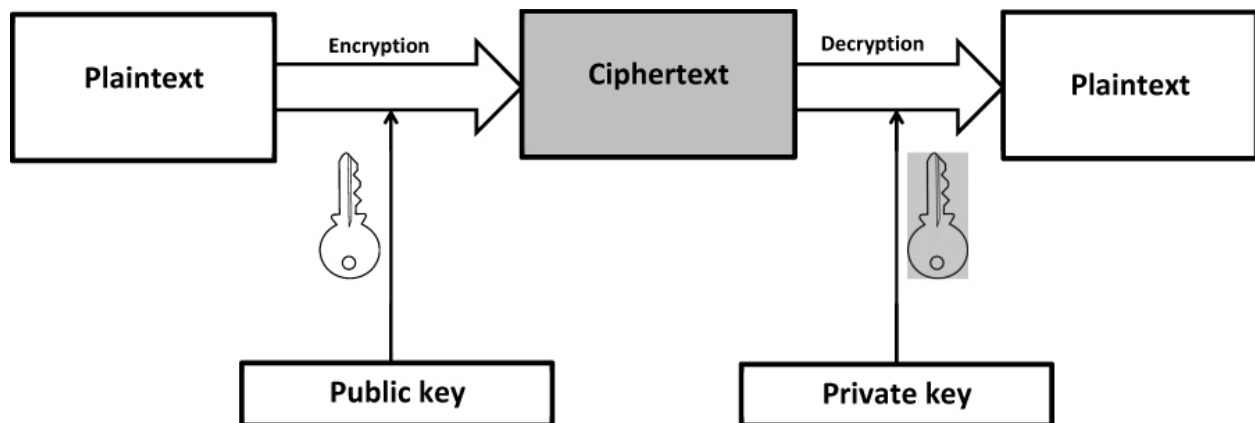


Fig4

In RSA every participant has the public key of every other participant, anyone can start an encrypted communication with anyone else (by using the other participant's public key). RSA prevents unauthorized logins, even when passwords have been compromised. Although AES is extremely secure and relatively fast but a common key is shared between parties which is a disadvantage and it causes more damage if compromised. AES or Advanced Encryption Standard Algorithm is Symmetric key

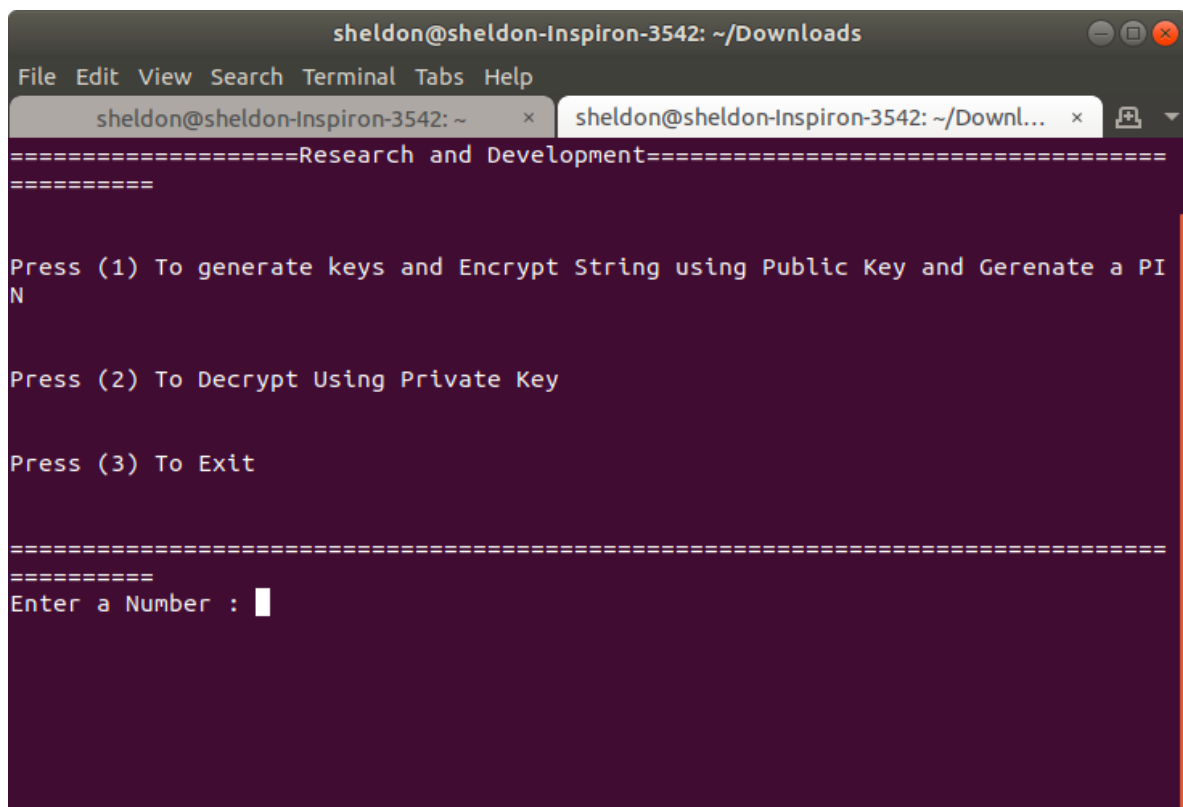
process. Both the parties possess of the same key, which is difficult to crack but once done.

### **How RSA-4096 bit encryption can be cracked?**

- Mathematically it is impossible to decrypt RSA encryption without knowing the key.
- For 4096 bit key encryption, the time may exceed the shelf life of the Milky Way Galaxy.
- Ways to exploit the vulnerabilities that exist in the implementation of the RSA encryption/decryption algorithm.
- This includes measuring variations in CPU voltage, noise produced by a device during encryption/decryption of a RSA encrypted message.

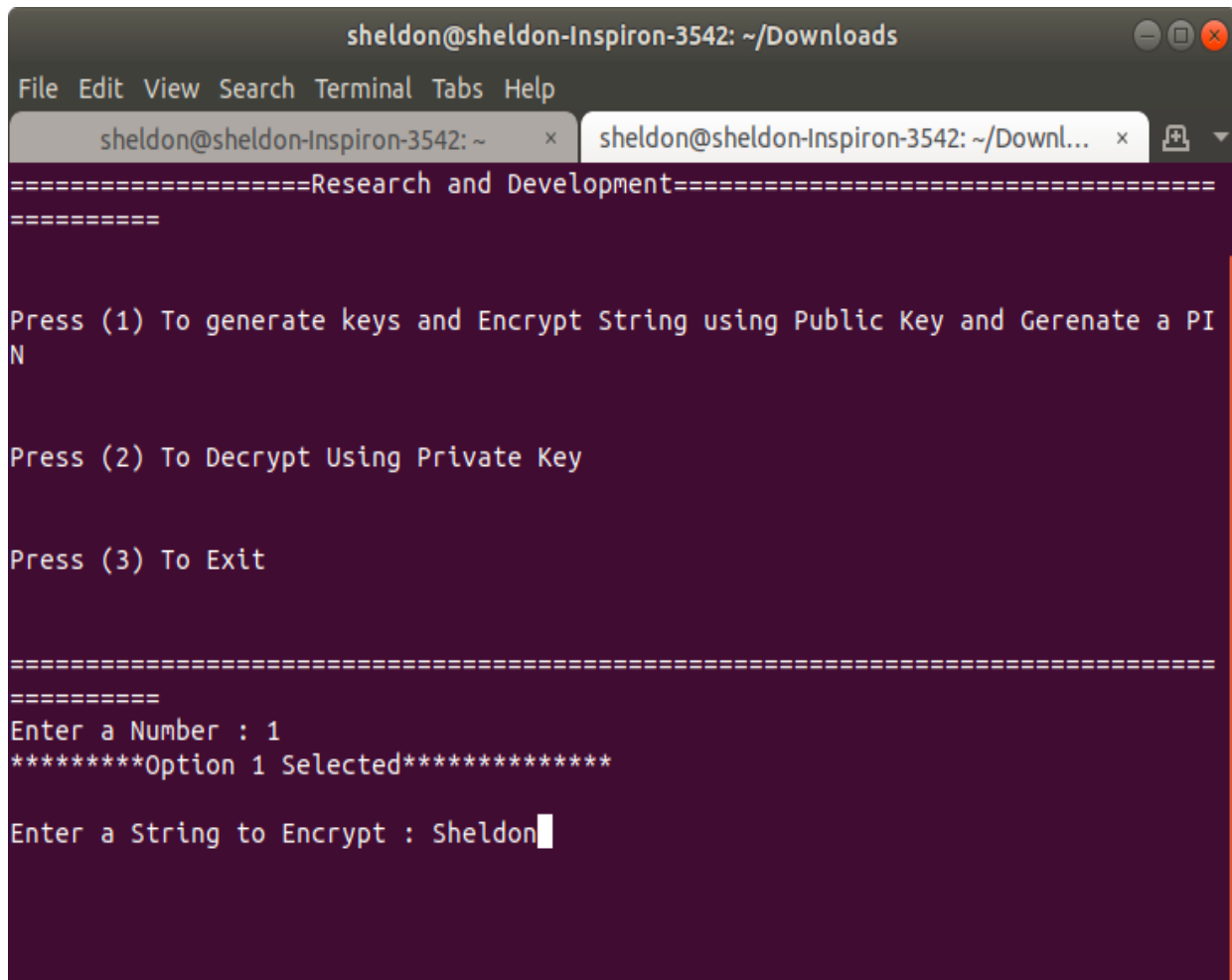
# Result

In our result we finally came up with a technology where we have used RSA-4096 as a prevention method against unauthorized attacks in social networking sites.



```
sheldon@sheldon-Inspiron-3542: ~/Downloads
File Edit View Search Terminal Tabs Help
sheldon@sheldon-Inspiron-3542: ~ x sheldon@sheldon-Inspiron-3542: ~/Downl... x
=====Research and Development=====
=====
Press (1) To generate keys and Encrypt String using Public Key and Gerenate a PIN
Press (2) To Decrypt Using Private Key
Press (3) To Exit
=====
=====
Enter a Number : 
```

Fig 5



The image shows a terminal window titled "sheldon@sheldon-Inspiron-3542: ~/Downloads". The window has a menu bar with "File", "Edit", "View", "Search", "Terminal", "Tabs", and "Help". There are two tabs open, both showing the same path. The terminal content is as follows:

```
=====Research and Development=====
=====

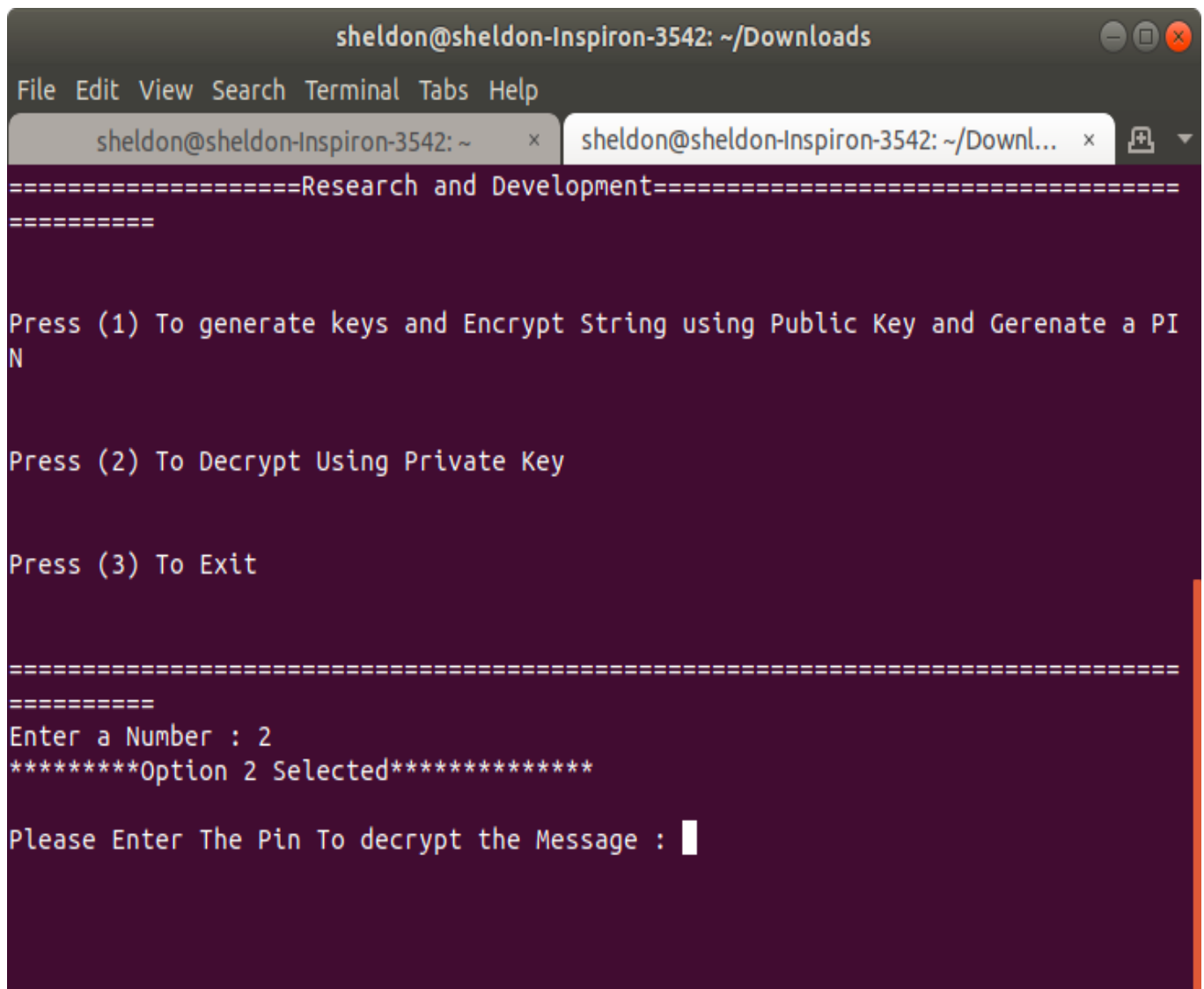
Press (1) To generate keys and Encrypt String using Public Key and Gerenate a PI
N

Press (2) To Decrypt Using Private Key

Press (3) To Exit

=====
=====
Enter a Number : 1
*****Option 1 Selected*****
Enter a String to Encrypt : Sheldon
```

**Fig 6**



The image shows a terminal window titled "sheldon@sheldon-Inspiron-3542: ~/Downloads". The window has a menu bar with "File", "Edit", "View", "Search", "Terminal", "Tabs", and "Help". There are two tabs open: "sheldon@sheldon-Inspiron-3542: ~" and "sheldon@sheldon-Inspiron-3542: ~/Downl...". The terminal content is as follows:

```
=====Research and Development=====
=====

Press (1) To generate keys and Encrypt String using Public Key and Gerenate a PI
N

Press (2) To Decrypt Using Private Key

Press (3) To Exit

=====
=====
Enter a Number : 2
*****Option 2 Selected*****

Please Enter The Pin To decrypt the Message : █
```

**Fig 7**

```
sheldon@sheldon-Inspiron-3542: ~/Downloads
File Edit View Search Terminal Tabs Help
sheldon@sheldon-Inspiron-3542: ~ x sheldon@sheldon-Inspiron-3542: ~/Downl... x
=====Research and Development=====
=====

Press (1) To generate keys and Encrypt String using Public Key and Gerenate a PI
N

Press (2) To Decrypt Using Private Key

Press (3) To Exit

=====
=====
Enter a Number : 2
*****Option 2 Selected*****

Please Enter The Pin To decrypt the Message : 650299
```

**Fig 8**

```
sheldon@sheldon-Inspiron-3542: ~/Downloads
File Edit View Search Terminal Tabs Help
sheldon@sheldon-Inspiron-3542: ~ x sheldon@sheldon-Inspiron-3542: ~/Downl... x
Please Enter The Pin To decrypt the Message : 650299

Reading Private.key
<_RSAobj @0x7f793b2051b8 n(2048),e,d,p,q,u,private>

Reading Encrypted Message
VNgnm2bH1Aojs6SksVtmQdQzHiKGPBUEEVTbQkhWrVXMwDvcfK+b2+zvKShknfbPW1v2Dp++0FKcYAg2
sdhnNKwXKkUb3b7UGsT3N/iS+hYuSVQK9lI1UsTYXl+rpsz/Y4jl7sSmrTjZkbln6TmD38Ppue8agsP7
TdoK+xQCRiFvyZxd4/VZ6imCOe/llHY9o0Lrps/3IUf/G+y0XaIAwkaYyHo5pw890WUef8ddj2Db8IRK
TtCLsI1TCof6R3khNQ+nPu2a0Se2kRXUgi99d79VRLIjvJwWcIDAXaTLJFjoioc1qbv9fnG9sKvrNt1j
j70/f0j8ZCZxIvxXtxB6gQ==

Decrypting Encrypted Message

Decrypted Message: Sheldon

Press Enter to continue...
```

Fig 9

# **SUMMARY**

- The project implemented describes identifying the authorized user of the social networking website. This particular algorithm implemented has a variety of uses in terms of building applications for teaching-learning processes, and can further be developed for implementing high security applications as well.
- The real world does not always include authentic user but also unauthorized user and therefore an approach to building an algorithm that could detect authentic user from unauthorized ones.
- Authorized user from real world were also authenticated using the above methods and also with the help of Trusted users method using 6 digit pin .
- Changes were made to the very first implementation of detecting user so as to differentiate authorized and unauthorized user of that particular account.
- The changes made were mostly by sending random generated pin of length 6 to the trusted contacts .
- Some of the part implemented also made use of RSA encryption technology. Using RSA, the OSA can generate a random string and encrypt it using the RSA. The private key of the RSA is send to the user and a 6 digit random generated pin is send to the Trusted contacts . The OSN will provide a platform where user have to enter the pin send to the Trusted contact and upload the private key file , only upon successful decryption of the random text the authenticity is proved.



# **Future Work**

- We have decided that we we'll be working on increasing the encryption by combining RSA with AES .
- We will be looking forward to make more user friendly interface and hence continue our research.
- Submitting a research paper on the very topic is something that the project members look eagerly forward to.

# **References**

- Novel authentication procedures for preventing unauthorized access in social networks, M. Milton Joe<sup>1</sup> & B. Ramakrishnan<sup>2</sup>
- Joe MM, Ramakrishnan B, Shaji RS (2013) Prevention of losing user account by enhancing security module: A facebook case. J Emerg Techol Web Intell 5(3):247–256
- Venkateswari P, Purusothaman T (2011) A secure simple authenticated key exchange algorithm based authentication for social network. J Comput Sci 7(8):1152–1156
- Aboud SJ (2010) Efficient password-typed key agreement scheme. Int J Comput Sci 7:26 –31, <http://www.doaj.org/doaj?func=abstract&id=495633>
- Joe MM, Ramakrishnan B (2015) Review of vehicular ad hoc network communication models including WVANET (Web VANET) model and WVANET future research directions. Wirel Netw 1–15. doi:10.1007/s11276-015-1104-z.