International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)
Web Site: www.ijettcs.org Email: editor@ijettcs.org
Volume 4, Issue 1, January-February 2015 **ISSN 2278-6856**

Privacy & Security a Concern in Social Networks

Aamir Suhial

Jamia Hamdard University, Department of Computer science,
Hamdard Nagar, Delhi 110062, India

Abstract

In the present generation, the social life of everyone has become associated with the online social networks. These sites have made a drastic change in the way we pursue our social life. Making friends and keeping in contact with them and their updates have become easier. But with their rapid growth, many problems like fake profiles, online impersonation have also grown. There are no feasible solution that exist to control these problems. In this paper, we have shown how these fake profiles are threat to the users & the social networking. How one can break the privacy of modern social networks by using fake profiles. i have provided a mechanism to stop creation of these fake profiles. Security has always been a concern in online social services I have proposed a security authentication for logging into the Online social networks .

1. INTRODUCTION

Online Social networking (**OSN**) has evolved at a rapid pace from past few years as people have shown good response by trusting these OSN. there are almost 100 million active users on social networks. While facebook , Twitter & Google are hitting the top slabs. most individuals desire to stay connected with friends family relatives and virtual friends.When people join social networking sites, they begin by creating a profile, then make connections to existing friends as well as those they meet through the site. A profile is a list of identifying information. It can include your real name, or a pseudonym. It also can include photographs, birthday, hometown, religion, ethnicity, and personal interest. Members connect to others by sending a "friend" message, which must be accepted by the other party in order to establish a link. "Friending" another member gives them access to your profile, adds them to your social network, and vice versa. Members use these sites for a number of purposes. The root motivation is communication and maintaining relationships.Popular activities include updating others on activities and whereabouts, sharing photos and archiving events, getting updates on activities by friends, displaying a large social network, presenting an idealized persona, sending messages privately, and posting public testimonials.People are busy in chatting ,making new friends, uploading photos , liking ,commenting & updating status etc. majority of the active users hardly think of privacy and security as they trust these OSN. Trusting has lead a common user privacy naked online . While disclosing information on the web is a voluntary activity on the part of the users, users are often unaware of who is able to access their data and how their data can potentially be used. how safe & private ones personal information is ?? Users on OSN has desires to meet different types of people from different parts of the world. A normal user enjoys time with them but is that stranger actually existing as per the information he/she has shared , it gives us an idea about fake profiles how safe is it to accept friend request of such types of users. How to stop these fake profiles ??.Security always plays a vital role on OSN it poses a threat to privacy of an users account. How secure online social networks are.??.

2. OVERVIEW

Nowadays, the web is all about Facebook, Twitter, YouTube, Tumblr. But seven years ago, all these services didn't exist, portals and search engines where still king. So what happened during this period? To make a long story short: users took the control of the web. Or, to be more accurate: the market shifted to a click-based engagement model to a fan-based engagement model. Which means, clicks are no longer the premium currency for advisers, fans are: they want to be followed, to be shared, to be mentioned, even to be pined! Fan is the new click.With the advent of user generated content and sharing features, social platforms are the new kings of the web. This being said, and I assume you already knew it, not every social platform are the same. Within the last seven years, we have been through three waves of social domination: The publishing wave (with blogs), the sharing wave (with Facebook and Twitter), and the curating wave (with Quora, Pinterest and alike). The main reason for this shift in users' behavior is the amount of content: the more content, the more precious it is to find the value-added content, this is why we are currently in the curating wave. The second reason is the evolution of users' expectations: the more they use social media, the more sophisticated their needs are. Thus, every six month, we are witnessing the arrival of "the new Facebook". But as you can experience it every day, we still have the same three dominant players (Facebook, Twitter, Google) and a dense ecosystem of niche players.

3. Social Impact:

In the present generation, the social life of everyone has become associated with the online social networks. These sites have made a drastic change in the way we pursue our social life. Adding new friends and keeping in contact with them and their up- dates has become easier.The online social networks have impact on the science, education, grassroots organizing, employment, business,

etc. Researchers have been studying these online social networks to see the impact they make on the people. Teachers can reach the students easily through this making a friendly environment for the students to study,teachers now-a-days teachers are getting themselves familiar to these sites bringingonline classroom pages, giving homework, making discussions, etc. which improves education a lot. The employers can use these social networking sites to employ the people who are talented and interested in the work, their background check can be done easily using this. Most of the OSN are free but some charge the membership fee and uses this for business purposes and the rest of them raise money by using the advertising. This can be used by the government to get the opinions of the public quickly. The examples of these social networking sites are sixdegrees.com, The Sphere, Nex-opia which is used inCanada, Bebo, Hi5, Facebook, MySpace, Twitter, LinkedIn, Google+, Orkut, Tuenti used in Spain, Nasza-Klasa in Poland, Cyworld mostly used in Asia, etc. are some of the popular social networking sites.

4. Statistics:

These online social networks are growing rapidly and there are more than 160 major social network websites exist in the world. 300 million active accounts in Facebook, The social networking sites are making our social lives better but nevertheless there are a lot of issues with using these social networking sites. The issues are privacy, online bullying, potential for misuse, trolling, etc. These are done mostly by using fake profiles.

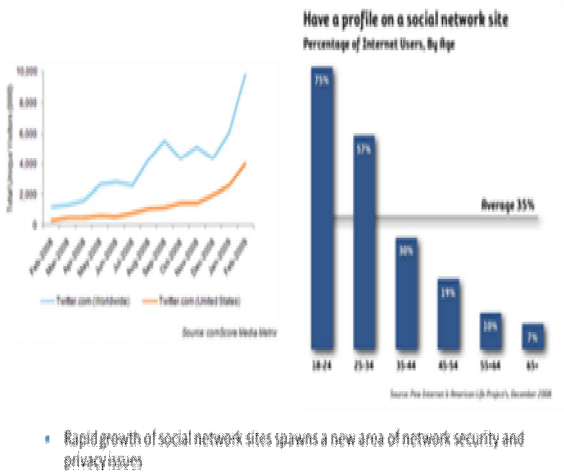


Fig 1:Rapid growth of social networks spawns a new area of network security & privacy issue

5. Literature Review

Fake profiles are the profiles which are not genuine i.e. they are profiles of persons who claim to be someone they are not, doing some malicious and undesirable activity, causing problems to the social network and fellow users.
Why do people create fake proflies ?
Social Engineering
Online impersonation to defame a person
Advertising and campaigning a person, etc

6. Social Engineering

Social Engineering in terms of security means the art of stealing confidential information from people or gaining access to some computer system mostly not by using technical skills but by manipulating people themselves in divulging information. The hacker doesnt need to come face to face with the user to do this. The social engineering techniques are like Pretexting, Diversion theft, phishing, baiting, quid pro quo, tailgating, etc. Eg: Creating a profile of some person X not in some online social networking site like facebook. Adding the friends of the X in facebook and making them believe that its the profile of X. They can get the private information meant for only X by communicating with Xs friends

Fig 2: shows the screenshot from yahoo news which shows the best example of social engineering done using an online social network facebook, in which some spies created a fake facebook account in the name of James Stavridis, the chief of NATO. They sent requests to many other officials in NATO and some officials in other important organizations and are able to extract a lot of important information

7. Online impersonation to defame a person

The other reason why people create fake profiles is to defame the persons they do not like. People create profiles in the name of the people they don't like and post abusive posts and pictures on their profiles misleading everyone to think that the person is bad and thus defaming the person.

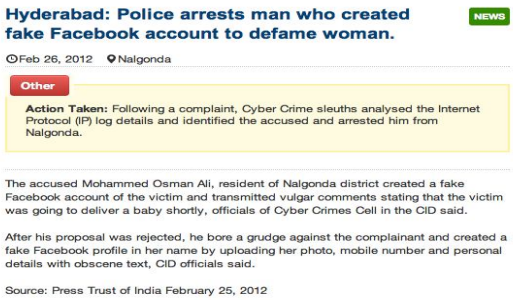


Fig3: shows the screenshot from a website which shows that a man named Mohammad Osman Ali has created a fake profile of a woman in facebook and tried to defame her. The police finally caught and arrested him. This shows a very serious problem existing now-a-days.

8. Advertising and Campaigning

Imagine a scenario where a movie is released and one of your friends in facebook posted that the movie was awesome. This makes a first impression on you that the movie is good and you would want to watch it. This is how advertising and campaigning works through OSN.The review posted by a genuine user is always desirable but these reviews when posted by fake profiles and completely undesirable.

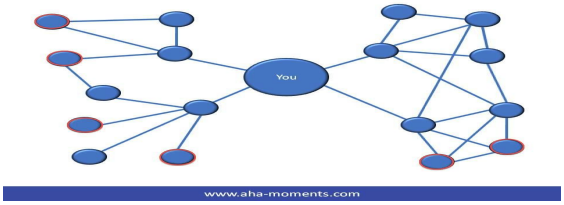


Fig4: Assume that Fig4 shows a social graph where the blue nodes shown are real profiles, the red circled profiles show fake profiles and the edges show the connections between them. If the fake profiles start advertising a brand or campaigning for some politician then the users connected to the fake profiles are misled in believing them. Inturn the profiles who didnt add the fake profiles are elected using the mutual connections.

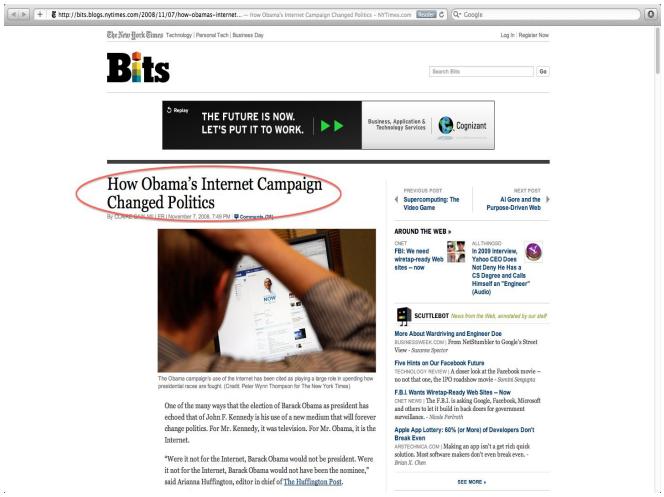


Fig5: Figure shows a screenshot, which shows the post in New york Times showing the most successful internet campaigning done by Obama which collected around 500 million dollars of election fund for him. Obama might not have used fake profiles in his internet campaigning but this shows the power of internet campaigning. Imagine a case where a non deserving candidate used this fake profiles to campaign. That is a very highly undesirable situation.

9. Social Bots

Social bots are semi-automatic or automatic computer programs that replicate the human behavior in OSN. These are used mostly by hackers now-a-days to attack online social networks. These are mostly used for advertising, campaigning purposes and to steal users personal data in a large scale.These social bots communicate with each other and are controlled by a program called Bot master. The bot master may or may not have inputs from a human attacker. The social bots look like human profiles with a randomly chosen human name, randomly chosen human profile picture and the profile information posted randomly from a list prepared from before by the attacker. These social bots send requests to random users from a list. When someone accepts the request, they send requests to the friends of the user who accepted the request, which increases the acceptance rate due to existence of mutual friends.Recently a researcher from university of british Columbia made a social botnet of 103 bots in facebook and added 3000 friends in just 8 weeks. He was able to extract around 250 GB of personal data of users. This shows the extent of the applications of social bots by the attackers.

10. Facebook Imune System(FIS)

When we consider facebook, it has its own security system to protect its users from spamming, phishing, etc. and this is called facebook immune system. FIS does real time checks on every single click and every read and write operation done by it. This is around 25 Billion checks per day and as high as 620,000 checks per minute at peak as of may, 2011.

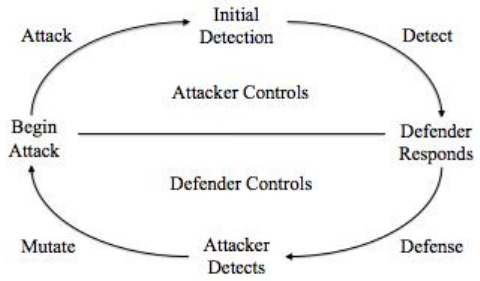


Fig6: shows the adversarial cycle in which the top part is controlled by the attacker and the bottom part shows the response by the FIS to control the attack, which when detected by the attacker, he/she mutates the attack and attacks it again. This goes on like a cycle and is never ending. FIS is able to detect the spam, malware and phishing produced by the compromised ad fake accounts. They are actually able to reduce the spam to less than 0.4 FIS is not successful in detecting the social bots and the fake accounts created by humans. This can be seen by the example mentioned above where a researcher created 103 social bots to collect a lot of personal data of users and facebook could not detect this attack.103 social bots to collect a lot of personal data of users and facebook could not detect this attack.

Proposed Work

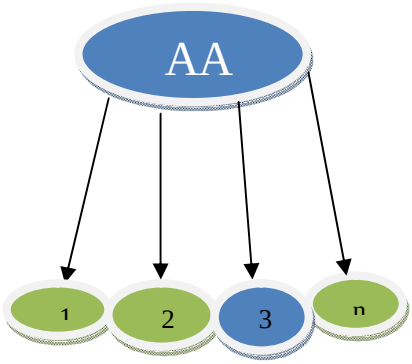
Privacy Analysis "Fake accounts threat to OSN"

As social networking sites have improved the privacy controls we will discuss about the worlds most popular OSN Facebook , it provides the users to customize the account privacies as per there choice like an unknown persons messages wont be delivered in the inbox , an

unknown person cant like comment or send friend request. Who can see you on social network that too is being customized such privacy controls are great to support the users privacy.

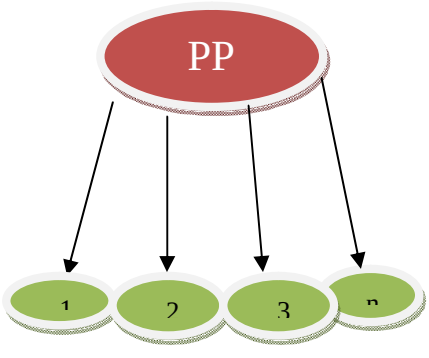
- We made an attempt to check how perfect these controls work. Lets say there is an account "AA" who has kept a privacy control to friends not public . AA has friends let us say X-friends. An Unauthorized person "pp" wants to track the personal information of the AA as the privacy is to friends only is not letting PP to send a friend request nor a message . person PP created a fake profiles by keeping some honey posts and sexy pictures it attracts most of the friends(teenagers) of the AA account lets say BB CC DD EE became friends with PP, as the number of mutual friends increased the PP was able to send the message as well as the friend request to "AA". That is how an personal information can be viewed and attacked despite of the fact that OSN has provided the privacy controls. In this paper we tried to show how much a fake account are threat to OSN . now the same way PP who created fake accounts can send request to AA from other accounts as well by increasing the count of mutual friends. PP has many fake profiles that is only known to PP, for AA they are different people PP can use these accounts to take a full control over the AA not only in the virtual OSN but It might affect the AA in the real life as well. PP can now act as chameleon on OSN he can chat from all the different fake accounts to the same person

Acount "AA" having privacy to friends



AA(n) n=friends of AA

PP Creating fake profiles:



PP(n) n=fake profiles of PP

Reason for creating fake accounts is only to increase no of mutual friends with AA

As the number of mutual friends increases PP will be able tosend request/message.

"PP" uses a simple steps to approach "AA"

Algorithm

Start

1-Create a new account

2-Confirmming an email address

3-Adding friends[AA(n)]

Is "PP" able to send request to "AA"
{
Send request/message
End
}
Else
{
Goto 1.
}

Worm attack:-A special malware worm is designed which create fake accounts . The most notorious worm in social network is the koobface. According to Trend Micro, the attack from koobface as follows:

Step 1: Registering a Facebook account.

Step 2: Confirming an e-mail address in Gmail to activate the registered account.

Step 3: Joining random Facebook groups.

Step 4: Adding "friends" and posting messages on their walls.

The popularity of the OSN is monitored on the basis of active users, facebook is clamming the numero uno spot . As per the 2014 "statisticbrain" survey

Table 1: 2014 "statisticbrain" survey

Facebook Statistics	Data
Total number of monthly active Facebook users	1,310,000,000
Total number of mobile Facebook users	680,000,000
Increase in Facebook users from 2012 to 2013	22 %
Total number of minutes spent on Facebook each month	640,000,000
Percent of all Facebook users who log on in any given day	48 %
Average time spent on Facebook per visit	18 minutes
Total number of Facebook pages	54,200,000

These increase in fake accounts actually gives false statistics of the OSN . The BBC repoted that on firms who are wasting money to gain "likes" from fake profiles and users who have no interest in their products: "A BBC investigation suggests companies are wasting large sums of money on adverts to gain "likes" from Facebook members who have no real interest in their products. It appears many account holders who click on the links have lied about their personal details. A security expert has said some of the profiles appeared to be "fakes" run by

computer programs to spread spam." Using number of likes to judge the success of a social media platform is a rudimentary method of analysis. While many senior managers still like to see vast numbers of likes on the company's Facebook page, this is more about vanity than effective engagement.

Teens are sharing more information about themselves on social media sites than they have in the past, but they are also taking a variety of technical and non-technical steps to manage the privacy of that information. Despite taking these privacy-protective actions, teen social media users do not express a high level of concern about third-parties(such as businesses or advertisers) accessing their data; just 9% say they are "very" concerned. These teens easily become the victims of honey posts created by these fake user it is being

Teens are sharing more information about themselves on their social media profiles than they did when we last surveyed in 2006:

91% post a photo of themselves, up from 79% in 2006.
71% post their school name, up from 49%.
71% post the city or town where they live, up from 61%.
53% post their email address, up from 29%.
20% post their cell phone number, up from 2%.
60% of teen Facebook users set their Facebook profiles to private (friends only), and most report high levels of confidence in their ability to manage their settings.

Teens are actively participating on OSN the attack happens by using the fake profiles to teens personal information. Which creates a further threat to the OSN as after using the privacy controls still users are being kept nacked or attacked online.

Security an issue in OSN:

How fake profiles are used to gain access over ones account:

Security has been a primary issue and a concern for every company various papers have been published on the security of OSN as users are trusting the companies. The scariest part is that as we get more comfortable with advances in technology, we actually become more susceptible to hacking. As if we haven't already done enough to aid hackers in their quest for our data by sharing publicly, those in the know can get into our emails and Facebook accounts to steal every other part of our lives that we intended to keep away from prying eyes.In fact, you don't even have to be a professional hacker to get into someone's Facebook account.

It can be as easy as running Firesheep on your computer for a few minutes. In fact, Facebook actually allows people to get into someone else's Facebook account without knowing their password. All you have to do is choose three friends to send a code to. You type in the three codes, and voilà—you're into the account. It's as easy as that. Various methods are there the most venerable way to attack viz

1)Phishing :

The first and very basic way of hacking Facebook accounts is via Phishing. Phishing is actually creating fake web pages to steal user's credentials like email,passwords,phone no,etc.

2)Keylogging :

This is another good way of hacking Facebook accounts. In this type of attack a hacker simply sends an infected file having keylogger in it to the victim. If the victim executes that file on his pc, whatever he types will be mailed/uploaded to hacker's server. The advantage of this attack is that the victim won't know that hacker is getting every Bit of data he is typing. Another big advantage is that hacker will get passwords of all the accounts used on that PC.

3)Trojans/backdoors

This is an advanced level topic. It consists of a server and a client. In this type of attack the attacker sends the infected server to the victim. After execution the infected server i.e. Trojan on the victim's PC opens a backdoor and now the hacker can do whatever he wants with the victim's PC

4)Sniffing

It consists of stealing session in progress. In this type of attack an attacker makes connection with server and client and relays message between them, making them believe that they are talking to each other directly.

5)SocialEngineering

This method includes guessing and fooling the clients to give their own passwords. In this type of attack, a hacker sends a fake mail which is very convincing and appealing and asks the user for his password. Answering the security questions also lies under this category.

6)SessionHijacking

In a session hijacking attack an attacker steals victims cookies, cookies stores all the necessary logging Information about one's account, using this info an attacker can easily hack anybody's account. If you get the cookies of the Victim you can Hack any account the Victim is Logged into i.e. you can hack Facebook, Google, Yahoo.

The easiest way to "hack" into someone's Facebook is through resetting the password. This could be easier done by people who are friends with the person they're trying to hack.

Simple Attack via Fake accounts

- The first step would be to get your friend's Facebook email login. If you don't already know it, try looking on their Facebook page in the Contact Info section.
- Next, click on **Forgotten your password?** and type in the victim's email. Their account should come up. Click **This is my account**.
- It will ask if you would like to reset the password via the victim's emails. This doesn't help, so press **No longer have access to these?**
- It will now ask **How can we reach you?** Type in an email that you have that also isn't linked to any other Facebook account.
- It will now ask you a question. If you're close friends with the victim, that's great. If you don't know too

much about them, make an educated guess. If you figure it out, you can change the password. Now you have to wait 24 hours to login to their account.

If you don't figure out the question, you can click on Recover your account with help from friends. This allows you to choose between three and five friends.

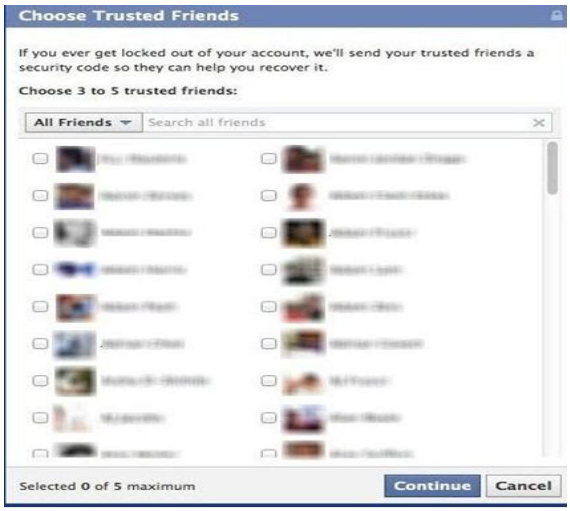


Fig-7: Screen shot of facebook privacy option

It will send them passwords, which you may ask them for, and then type into the next page. You can either create three to five fake Facebook accounts and add your friend (especially if they just add anyone),

Fig-8:screen shot of security code window in FBK

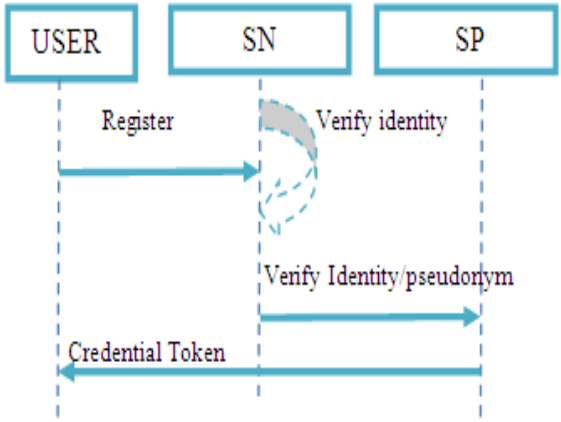
The security compromise can lead to the fear in the users that their accounts are not safe on OSN that is the threat to the future of both the privacy of users and the long lasting fashion of OSN .

Password cracking is one of the famous ways to break the security by just following the forgot password link and answering few question as the technology advanced now the OSN has come with more secure ways but still accounts are hacked or the original users control is bypassed in some cases when an account is hacked the users email account is even removed from the profile the original user have no way to gain back the control over their accounts. Some of the mishaps is that these hackers even upload the nude pictures as the display picture of the particular prey. There should be a proper mechanism for both the privacy and security of the users.

Solution: Stop creation of fake Accounts: As we showed and discussed the threat of fake profiles to OSN We will purpose a simple and easy ways to stop the creation of fake accounts. There should be a mechanism that ones identity is know before he/she can claim the part of social networks

1) Mobile number authentication

OSN should generate and sent an account creation code as an sms to that number to prove an identity of an individual before creating an account there should be a mandatory mechanism and the option for user to use their mobile number as the primary key to prove his identity or in other terms user authentication. When a user enters his mobile number social networks generate an authentication code (token),That token is being sent to the Mobile service provider then service providers deliver the token on the users screen. Now the user can type the received code on the particular OSN .hence this type of authentication is quite simple and accurate



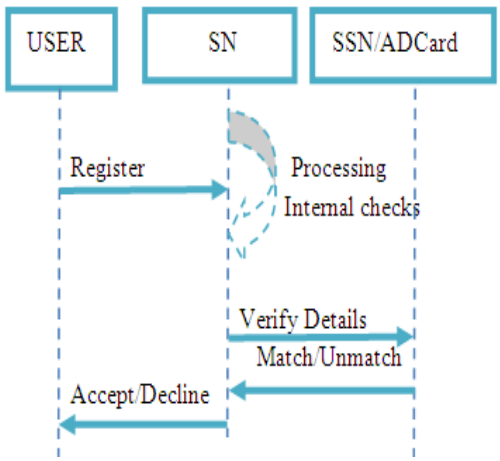
Registration process i

Step 1: Sign up/enter your details
Step 2: Enter you valid mobile number
Step 3:Server generated a token(can use OTP) Sent on the mobile number
Step 4:x=Enter a token number

```
If(x==token)
{
 Print User registered
   }
 Else
{
   Goto step 3
}
```

2) Social security number or Adhar number

If any one cant prove his identity using his mobile number than He/she should have a an option to choose his primary and unique Social security number or Adhar number there should be proper checks that the information mentioned on the OSN is matching to the information that is regester for particular Social security number or Adhar number. Hence we can not only stop fake profiles but multiple accounts as well.



Registration process ii

Step 1: Step 1: Sign up/enter your details
Step 2: Enter you Social security number/Adhar number
If number already exists in OSN
{
Already a Registerd user
}
Else
{
Check details of user matches the Social security number/Adhar number data base
If matched
{
Welcome
User registered
End if
}
Else
{
Goto Step 2;
}

Identity proof:if the users are not able to prove their identity in any way then they should be able to send the softcopy of the registered govt approved identity proof to the OSN sites. Like passport/ driving licence/voter id card/pan card etc

Retina Scan: As the modern devices like computers and smartphones are blessed with the high quality cameras both primary and secondary . OSNs should be able to check the identity of a person by just retina scan using the camera of the particular device that a account holder is using.

Finger print recognition: As the advanced improvement in technology has given us multiple ways to prove the identity of a particular person the modern devices like computers or smart phones have an inbuild finger print recognition Apple iphone 5s and almost on evry modern micro computer.

The above mentioned solutions would not completely guarantee the fake free OSN but we will be able to stop a lot of fake account creation. In future there might come an advanced technology as it is growing at a rapid pace those new technologies can be implemented to secure the the OSN. hence there is a lot of future research.

Solution to the security :

Authentication mechanism*:*As the modern technologies are supported with latest and secure encryption mechanism which actually makes it secure for users and for the OSN companies to keep the users credentials in a secure way. The passwords are stored in an encrypted form in the database of the particular OSN these encryptions can be decrypted and chances are that hackers are able to break into the targeted account. In order to make the account logins secure we are coming up with the security proposal as When a user is creating an account for first time. OSNs should maintain the database of customers login details like the ip address and the mac address , next time when a user logs in there should be a proper check of the last login ip and mac address if the details match the last login details then the normal security should be applied

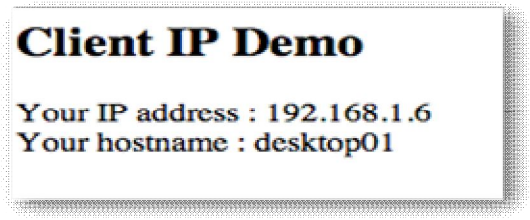
We can easily check the ip address in php as

```
$ip = $_SERVER['REMOTE_ADDR'];
```

Or

```
<?php
// client-ip.php : Demo script
// get an IP address
$ip = $_SERVER['REMOTE_ADDR'];
// display it back
echo "<h2>Client IP Demo</h2>";
echo "Your IP address : " . $ip;
echo "<br>Your hostname : ". gethostbyaddr($ip) ;
?>
```

Sample output



But if the credentials vary then the OSN should use LEVEL 2 security as google is using for that particular users have to activate the services Level 2 security is one in which an login code is generated and sent on the particular users registered mobile number. Now if the user does not have a mobile number registered than the security should come up with the further details like previous password and few other security questions like last 3 digits of bank account etc by these ways we can improve our security of being attacked by any online hacker. While OSN are able to authorize the particular user they should keep the newly mentioned credentials of the user stored in the database and should also email the details of the last login into the email address like

facebook has such type of privacy control that gives users to see the last login details.

If
New user then
{
Authenticate his identity
Store the x=current ip address and mac address
}
If
old user then
If (Current ip==x)
{
Welcome
}
Else
{
Level 2 security authentication
X= ip address and mac address
}

Future Work

As the proposed system can be used to to make the online social networking more easy more private more authentic and more secure. There is always a future scope of research as technology has been improving at a drastic speed. We need to develop or work on the complete fake free online social networking where we should not only be able to stop them but even detect and cancel them if they are existing.

11.CONCLUSION

This study focused on the importance of protecting social network users' personal information. It examined users' awareness of the risks and threats to their personal information privacy, and highlighted the need to develop a new privacy system supported by mobile Internet devices.

OSN companies should use any Trust factor algorithm to check the history of the user before he/she can send a friend request to any User making their life quiet secure simple and private.

The method of selecting privacy settings should also be simplified to provide users with a clear picture of the data that will be shared with others.

Although there is no standard for controlling personal information privacy settings, it is recommended that social network providers design a system which protects users from different types of threats and risks. Privacy systems of online social networks, especially those which areused for selecting personal information settings, can be improved in several ways. Controlling privacy settings from different types of internet mobile devices and supporting various screens sizes for these devices, will help users to control their personal information privacy settings easily in different places and times. Furthermore, using a predictable wizard system for setting privacy settings is a suggestion to support different Internet mobile devices and different screen sizes of mobile phones. In addition, privacy systems should inform users about which items of personal information are displayed and which are not.

REFRENCES

[1] T. Stein, E. Chen, and K. Mangla. Facebook immune system. In Proceedings of the 4th
[2] Workshop on Social Network Systems, SNS, volume 11, page 8, 2011.
[3] Y. Boshmaf, I. Muslukhov, K. Beznosov, and M. Ripeanu. The socialbot network: when botssocialize for fame and money. In Proceedings of the 27th Annual Computer Security Applications
[4] Awareness, Information Sharing, and Privacy on the FacebookPre-proceedings version. Privacy Enhancing Technologies Workshop(PET),2006
[5] IEEE Int'l Conference on Computational Science and Engineering, Vancouver,Canada, pp. 975-978. DOI 10.1109/CSE.2009.438 Privacy in Online Social Networking at Workplace
[6] IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 6, No 3, November 2011 ISSN (Online): 1694-0814
[7] A Survey of Security and Privacy in Online Social Networks Ed Novak Qun Li Department of Computer Science The College of William and Mary
[8] A. Fast, D. Jensen, and B. N. Levine. Creating social networks to improve peer-to-peer networking. In KDD, pages 568{573, 2005.
[9] X. Ying and X.Wu. On link privacy in randomizing social networks. In PAKDD, 2009.
[10] B. Zhou, J. Pei, and W.-S. Luk. A brief survey on anonymization techniques for privacy preserving publishing of social network data.SIGKDD Explorations, 10(2), 2009.
[11] Alessandro Acquisti and Jens Grossklags. Privacy and rationality inindividual decision making. IEEE Security and Privacy, 3(1):26 – 33, January/February 2005
[12] International Journal of Security, Privacy and Trust Management (IJSPTM) vol 2, No 2, April 2013DOI : 10.5121/ijsptm.2013.2201 1 PERSONAL INFORMATION PRIVACY SETTINGS OF ONLINE SOCIAL NETWORKS AND THEIR SUITABILITY FOR MOBILE INTERNET DEVICES
[13] International Journal of Science and Research (IJSR), India Online ISSN: 2319-7064 Volume 2 Issue 5 , May 2013 A Survey on Security Issues and Concerns to Social
[14] Literature Overview - Privacy in Online Social Networks Michael Beye1, Arjan Jeckmans2, Zekeriya Erkin1, Pieter Hartel2, Reginald Lagendijk1 and Qiang Tang2
[15] PRIVACY IN SOCIAL NETWORKS: A SURVEY Elena Zheleva Department of Computer Science University of Maryland College Park, MD 20742, USA
[16] A. Acquisti and R. Gross. Predicting social security numbers from public data. In PNAS, 2009.
[17] ENISA, "Security Issues and Recommendations for Online Social Networks,"Position Paper, Nov. 2007;

http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_social_networks.pdf
[18] The Failure of Online Social Network Privacy Settings_Michelle Maritza Johnson Steven M.
[19] Berkman Center for Internet & Society Teens, Social Media, and Privacy: New Findings from Pew and the Berkman Center
[20] A study of user authentication using mobile phone By Steffen Gullikstad Hallsteinsen
[21] 2011 International Conference on Communication Systems and Network Technologies . Token Based Authentication using Mobile Phone.
[22] Spies create fake facebook account in nato chief's name to steal personal details, http://in.news.yahoo.com/spies-create-fake-facebook-account-nato-chiefs-name-114824955.html.
[23] Man arrested for uploading obscene images of woman colleague http://www.ndtv.com/article/andhra-pradesh/man-arrested-for-uploading-obscene-images-of-woman-colleague-173266.
[24] How obamas internet campaign changed politics,/bits.blogs.nytimes.com/2008/11/07/ how-obamas-internet-campaign-changed-politics.

AUTHOR

Aamir Suhial received the M.S. degree in Computer Sciences from Jamia Hamdard University. & B.C.A. from University of Kashmir.