Enhancing Security Module to Prevent Data Hacking in Online Social Networks

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

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

***Abstract*—Online Social Network (ONS) is the easiest platform to connect with one another. There are many Online Social Networking websites exist to bring up the reliable communication among the users. Facebook, Orkut, Google+, Twitter, MySpace, etc are some of the Online Social Networking websites. All the social networking websites provide the interface formally known as profile, to share their willingness with others. The users of these websites could share their feelings, photos, text file and even whatever the user wishes to provide. All the Online Social Networking websites bring the friends, family members and relatives together to share their desires in a fast track manner, however still it lacks in security module. The shared photos and information are freely open access to all the users of social networking websites. When the photos are freely available, the unauthorized users can easily access the photos of others and download it. Once the photo is downloaded, that image can be misused widely such as creation of fake profile and the photo can be sold to other nuisance websites. This kind of data hacking activities in online social networks even leads the life to death. In this paper, data hacking in online social network is considered and a novel mechanism is presented to prevent the data hacking.**

***Index Terms*—Online Social Networks (OSNs), Internet, Security, Hacking, Data.**

I. Introduction

Internet is the web based communication tool, which brings all the users together and forms network communication to share the information with one another. Internet is the fastest and easiest technology to connect with people for communication [1]. Social networking is a service offered to form a network or relation to exchange the ideas, thoughts, interests, activities, backgrounds and so on [1, 2]. The research development in web 2.0 was very much useful to develop this sort of network communication and founded the Online Social Networks (OSNs) [1, 3]. The existing social networking websites such as Facebook, Orkut, and Google Plus and so on allow its users to create profile to post their ideas, activities and photos on the social networking websites. This profile can be viewed by the others users. These social networking websites help a lot to communicate with one another and get back the response for the post from the other users at once. The registration to create a profile in the social networking websites could be done with the help of existing E-Mail id [2]. Active users of social networking websites almost crossed more than one billion [2, 4, 5]. Though many social networking websites exist in the world, very few could stand among the people. One among them is the most popular social networking website Facebook, which crossed over one billion user during the month of September 2012. Most of the users use mobile device to access the social networking websites [6]. The recent survey says, the users of these websites by site wise as follows [7]:

• Facebook	: 1150 M (1.15 Billion)
• Twitter	: 500 M
• Google Plus	: 500 M
• LinkedIn	: 238 M
• Instagram	: 130 M
• Pinterest	: 70 M

The Figure 1 shows the overall total number of users presents in the social networking websites. The figure indicates clearly that Facebook has the highest number of users compared with all the other social networking websites. Using all the social networking websites, the users can present their day to day activities, photos and their life styles in their profiles. Friends, Family members, Relatives and even others can have a look at these profiles and they can respond back as they wish. The growth of social networking websites are developed every day, since many users create new profile every day. Thus, online social networking websites are widely used as a communication medium to share and exchange information with one another. The users are very much interested and spend most of their valuable time in social websites to exchange the information in a fast track manner.

doi:10.4304/jetwi.6.2.184-191

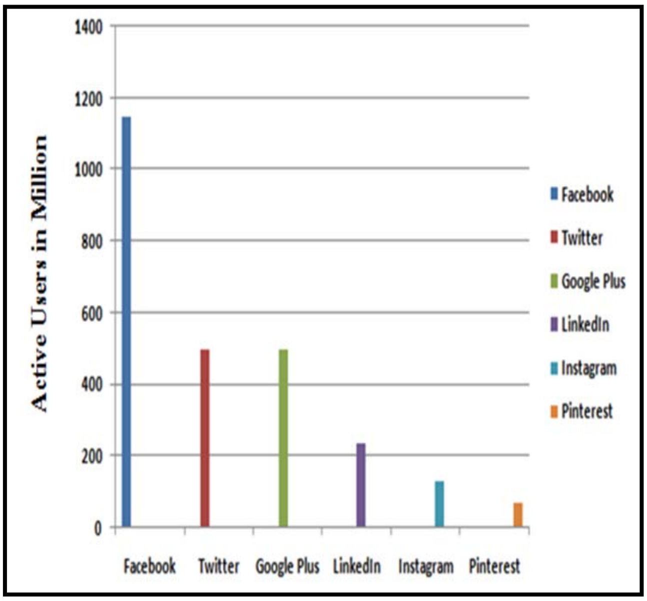


Figure 1 Total User of Social Network Websites

II. Related Work

Online Social Networking is one of the major areas, where so many researches have been taken for the development of social networking websites. Some of the research works done on social networking medium are listed below: When all the information are posted on Online Social Networking websites, privacy must be provided by the OSN providers. Privacy settings can be set by the users, those who are aware of the security constraints in social networking websites [8, 1]. The growth of the Online Social Networking websites laid the foundation for the development of third party applications to access the social networking websites' data to provide better performance to the users. Since user data are shared with third party applications, privacy to the user data must be provided. A separate framework was developed for third party applications for accessing the data from the user profile [3, 1]. That is, the user can set which data to be shared with third party applications [3, 1]. This framework set some sort of privacy to the user data in social networking websites.

The concern of privacy on user data developed a new framework, which made both OSN providers and non-friends to a particular user unable to access the user data [9]. Approach called FlyByNight employs the mechanism of cryptography, which never sends the data on social networking websites in an unencrypted format [10]. This FlyByNight brings up the data confidentiality over the online social networking websites [10]. Encryption techniques used to ensure the data confidentiality from the OSN provider in the approach of FaceCloak [11]. The FaceCloak mechanism provides equal access to all the friends of a particular user and no separate privacy is set for each friends of a particular user [11]. NOYB approach used cryptographic techniques to achieve the confidentiality from the OSN providers [12]. However the NOYB does not offer any tool for classifying the different permissions for each friend of a particular user [12]. Persona methodology offers a private OSN framework, which allows users to share their data with group of people securely defined by the user and Persona does not trust the OSN providers [13]. Lockr provides a new flexible data sharing method in a confidentiality manner in such a way the shared data cannot be accessed by the unauthorized users in Online Social Networking websites [14, 15].

All the social networking websites are threatened by the cyber criminals, who attack the social networking platform and breach the privacy of the users [16]. Socialbot is a software developed to control the attack on OSN platform [16]. Another vital challenge in Online Social Networking is preventing it from the worm propagation. The worm classified as muffle worm automatically propagates in the online social networking from one host to another host and infects it [17]. This muffle worm scans all the hosts in the social networking communication environment and identifies the vulnerable host among them [17, 18]. Once vulnerable host is identified the worm moves to that host and infects it and this process continues [17, 18]. The mechanism to detect such muffle worm and prevent the communication in online social networks securable is presented in the framework of muffle worm detection [17, 18]. All the above research works presented the mechanism of providing security to the user privacy and user data.

III. Problem Statement

The ideal growth of internet technologies developed Online Social Networks (OSNs) to communicate with others in an easiest manner. However to use the service of online social networks, user must register and create the profile. The user can post whatever he/she wants and the posted content is available to the other users. The other end user can view the post and reply back or comment on the post. Similarly most of the users post their original photographs on the social networking websites. Making the photographs available on the social networking websites are users own wish. As user's photographs are available on the websites, those photos can be easily hacked by the other users. These hacked photos are being misused widely, such as creation of fake profile, and for other bad activities. There are many ways to hack the data especially photographs on the social networking websites. So many people's life became a question mark because of the misuse of the photographs and even this lead to the death of lives. Prevention of this data hacking persists as a great challenge to the researchers

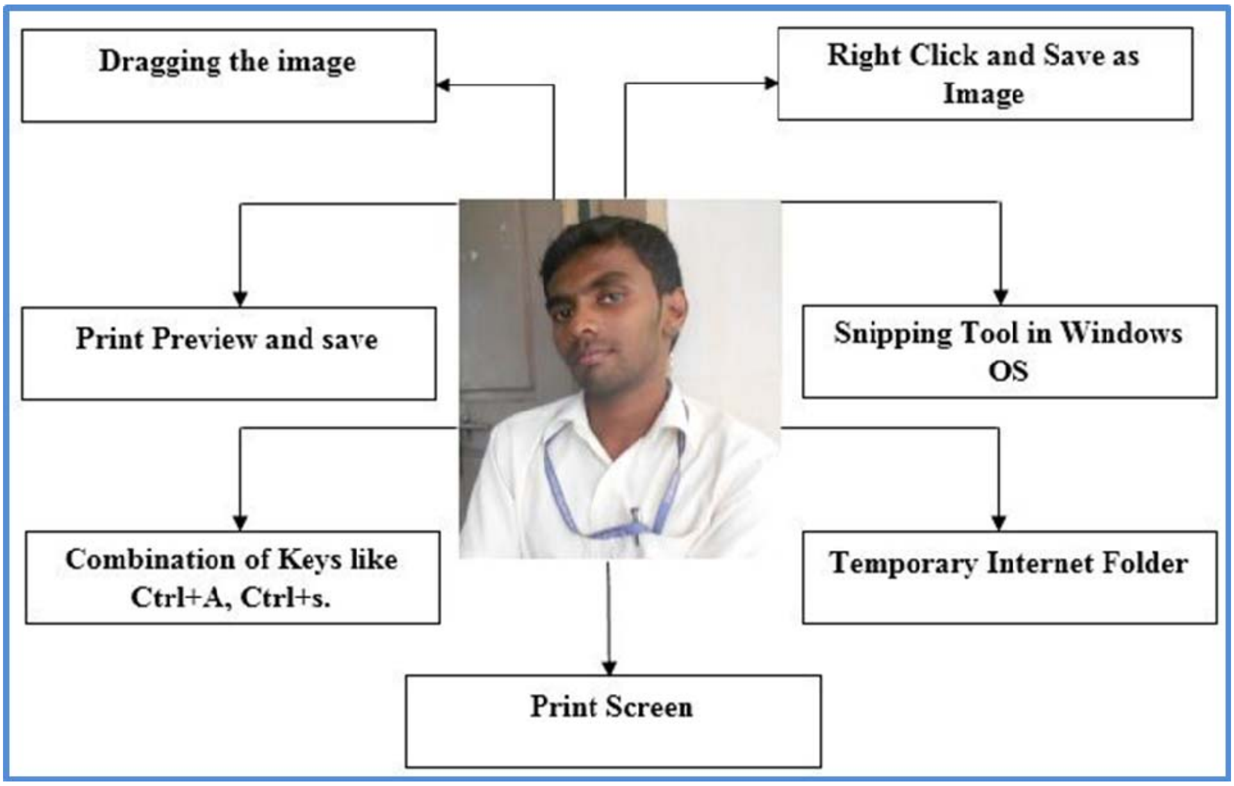

Dragging the image
Right Click and Save as Image
Print Preview and save
Snipping Tool in Windows OS
Combination of Keys like Ctrl+A, Ctrl+s.
Temporary Internet Folder
Print Screen

Figure 2 Ways of Hacking Photograph

The Figure 2 depict the various ways of hacking a photograph on social networking websites. There are five ways to hack an image in the websites as shown in the Figure 2. However to enhancing the security to the users on the social networking, this data hacking ways must be prevented. This data hacking made many people not to use the facility of social networking websites and also many people are not at all aware of these kind of data hacking. This paper concentrates on data hacking in social networking websites and a novel mechanism is presented to prevent the data hacking.

IV. Prevention Of Data Hacking

A. Disabling Right Click Option in OSNs

One of the ways of hacking the photograph in social networking website is right click and save image option. This option is find open in most of the social networking websites, which is very easy to download and save the images of others. This option must be disabled on social networking websites, in order to provide good security to all the social networking website users.

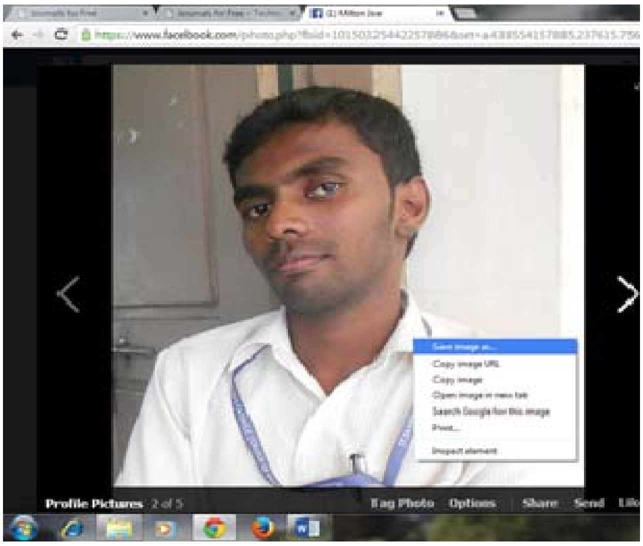
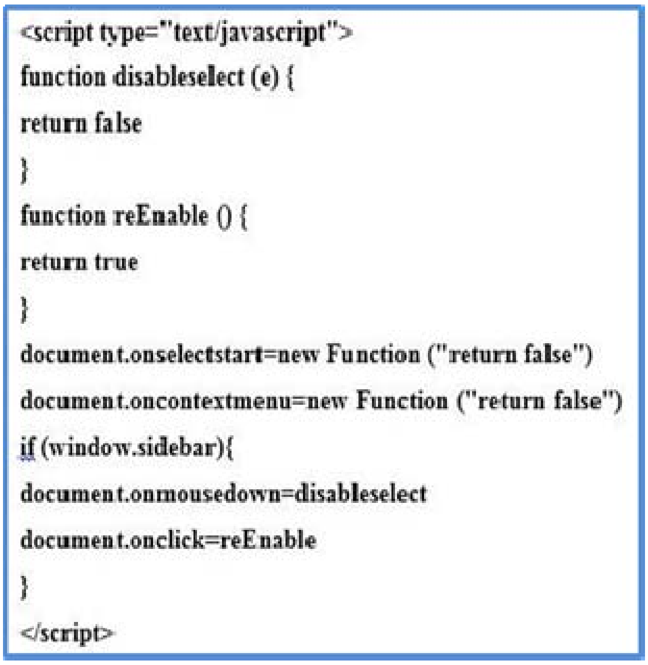


Figure 3 Right click and Save image

The above Figure 3 shows, how an image can be saved to the desktop in online social networking websites. It is a simple task to prevent the right click option in the social networking websites. The powerful Java script coding can be used to disable the right click option in the social networking websites.

The Java script code described below disables the right click option in any web pages. However, right click option may be needed in the web pages for ease of service. This paper proposes that this Java script code could be included in the social networking websites, in order to prevent the hacking of images without the knowledge of the intended user. Hence, inclusion of the Java script code enhance the security module in the social networking websites. Once security is improved, many people will make use the services of the social networking websites without any threat.



```
<script type="text/javascript">
function disableselect (e) {
return false
}
function reEnable () {
return true
}
document.onselectstart=new Function ("return false")
document.oncontextmenu=new Function ("return false")
if (window.sidebar){
document.onmousedown=disableselect
document.onclick=reEnable
}
</script>
```

Another way of hacking the image is dragging. User can easily drag the image to the any location where he/she wants to save the image. This dragging of the image is found open in online social networking websites.

Figure 4 represents how an image is dragged in Facebook social networking website. In the figure, we can find the same image in small size, when the image is being dragged. This dragged image can be dropped anywhere in the computer system for saving the image. This way of dragging an image must be disabled in order to tighten security constraint in social networking websites.

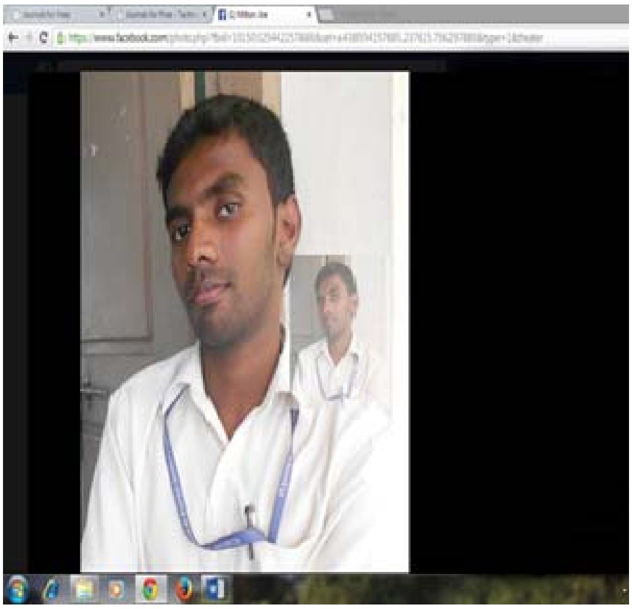


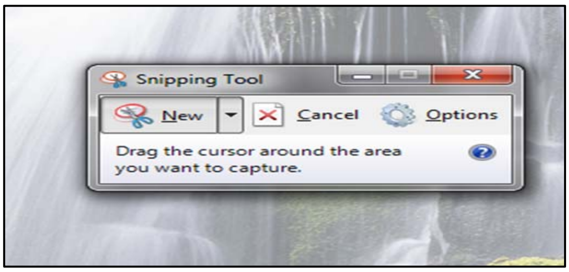
Figure 4 Dragging the Image

```
<img draggable="false" src="image.jpg" />
```

The tag <img> is used to display the image files in the webpages. This <img> tag has the attribute “draggable”, which returns the Boolean value that is either “true” or “false”. By default the value of “draggable” attribute is “true”. If the value of “draggable” attribute set as “false” as shown in the above <img> coding, then the image cannot be dragged. Hence this coding prevents the image dragging in social networking web pages.

C. Snipping Tool in Windows OS

Windows operating System such as Windows 7 offers a tool called Snipping tool. This tool can be used to take a copy of the image from the social networking web pages and the image can be saved in the desired location. The Figure 5 depicts the snipping tool. In the snipping tool, when new option is chosen, the mouse pointer is enabled to crop the image. Once the image is cropped, then user can save the image in the desired location. Using this snipping tool any image can be cropped and saved. This snipping tool option needs to be eliminated to enhance the security modules in social networking websites.

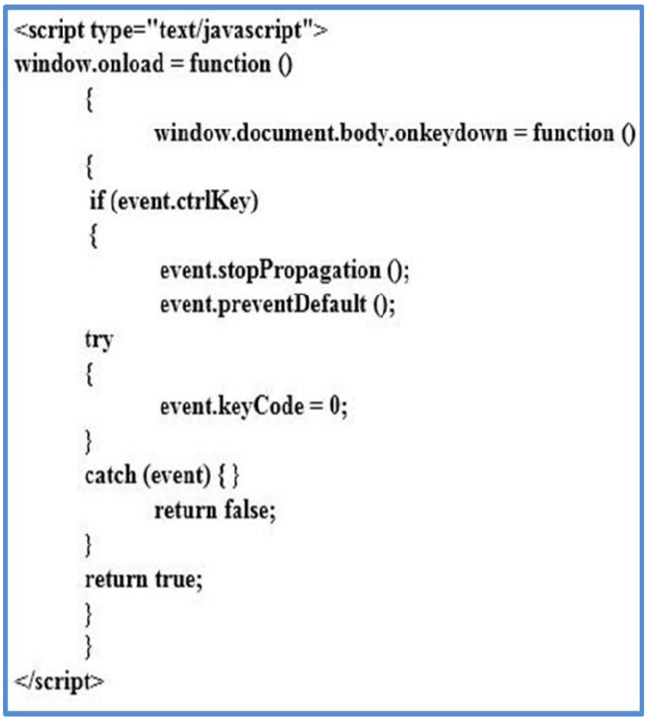


Drag the cursor around the area you want to capture.

Figure 5 Snipping tool to save the image

D. Combination of Keys

Image can be hacked with combination of key such as Ctrl +A and Ctrl +S. Disabling right click will prevent the hacking from the mouse operation. However once mouse operation is disabled, it is still possible for the hackers to copy the image with the Ctrl +A and Ctrl +C keys. When the user presses the above mentioned key combination, the entire current working environment is get selected. Once the working environment is get selected the key combination Ctrl +C could be used to copy the entire page and that can be pasted with the key wherever the user wants. In order to prevent data hacking in online Social networking webpages this Ctrl +A must be disabled. Similarly the key combination Ctrl +S allows users to save the current viewing web page as it is. When a web page is saved, all the images of the web page are saved in a folder for the ease of the hackers. Hence, this combination of Ctrl +S keys must be disabled in online social networking websites to enhance the security module.



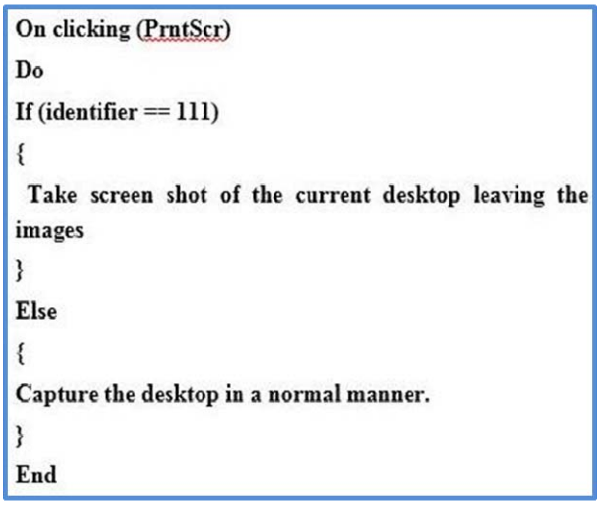
```
<script type="text/javascript">
window.onload = function ()
        {
                window.document.body.onkeydown = function ()
        {
        if (event.ctrlKey)
        {
                event.stopPropagation ();
                event.preventDefault ();
        try
        {
                event.keyCode = 0;
        }
        catch (event) { }
                return false;
        }
        return true;
        }
        }
</script>
```

The above placed java script code should be added in all the social networking web pages. This java script code disables the Ctrl + A, Ctrl + S and all the other keys with combination of Ctrl key. Implementation of these codes in social networking web pages prevents the user data highly and users will be saved from the threat of data hacking.

E. *Print Screen Option*

Print Screen option in computer system's keyboard provides good facility to all the researchers and others to take the screen shot of the current desktop position as it is. Similarly this print screen button (PrntScr) can be used to capture the screen in the Online Social Networking websites. Once the social networking webpage is captured that can be saved and cropped to have the image separately. Enhancing security constraint in social networking websites this Print Screen operation in the computer system needs to be disabled. However the usage of Print Screen option is much needed to all the users of the computer system. Hence this feature cannot be disabled. Alternatively this paper provides the novel mechanism, when the Print Screen button is pressed to capture the screen.

The novel mechanism is, assigning the same identifier to all the social networking websites. Similarly whenever a new social networking website is about to be created, the same identifier must be assigned to it also. For instance let us consider the key 111 is assigned to all the social networking websites. The working principle of Print Screen button in Online Social Network websites are described below. When the PrntScr button is pressed, it will check for the website's identifier. If the identifiers is equals to 111, then the screen shot will be taken without capturing the images found in the webpage. That is, except the image file all the other information will be captured. Similarly if the identifier is not equal to 111, then no restriction is given and the PrntScr option will function as it is. That is, all the contents of the screen is captured.



```
On clicking (PrntScr)
Do
If (identifier == 111)
{
 Take screen shot of the current desktop leaving the images
}
Else
{
Capture the desktop in a normal manner.
}
End
```

These days the hackers are much clever. When the proposed scheme is implemented, hackers will open a small working environment near the social networking web pages and take the print screen of the desktop. Along with the active window the social networking web page is also captured, since the print screen button will check the identifier of the active window. The Figure 6 depicts how an online social networking web page can be captured by making another working environment as active window. This way of hacking must be prevented to tighten the security constraints. Additional intelligence should be given to the print screen button, when it is being pressed. Whenever the print screen button is pressed, it must check how many windows are maximized. If more than one window is maximized, then it must prompt to minimize all windows by keeping one window as active. This checking will keep only one window active at a time. Hence the proposed mechanism will work perfectly.

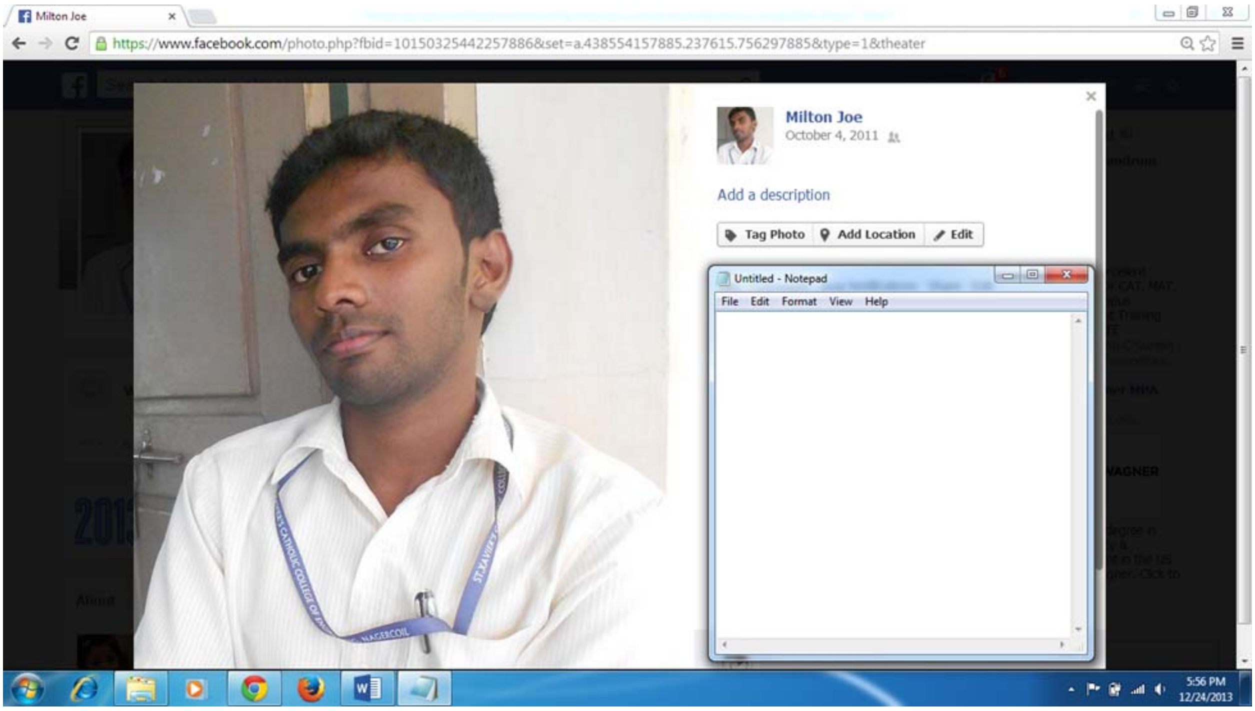
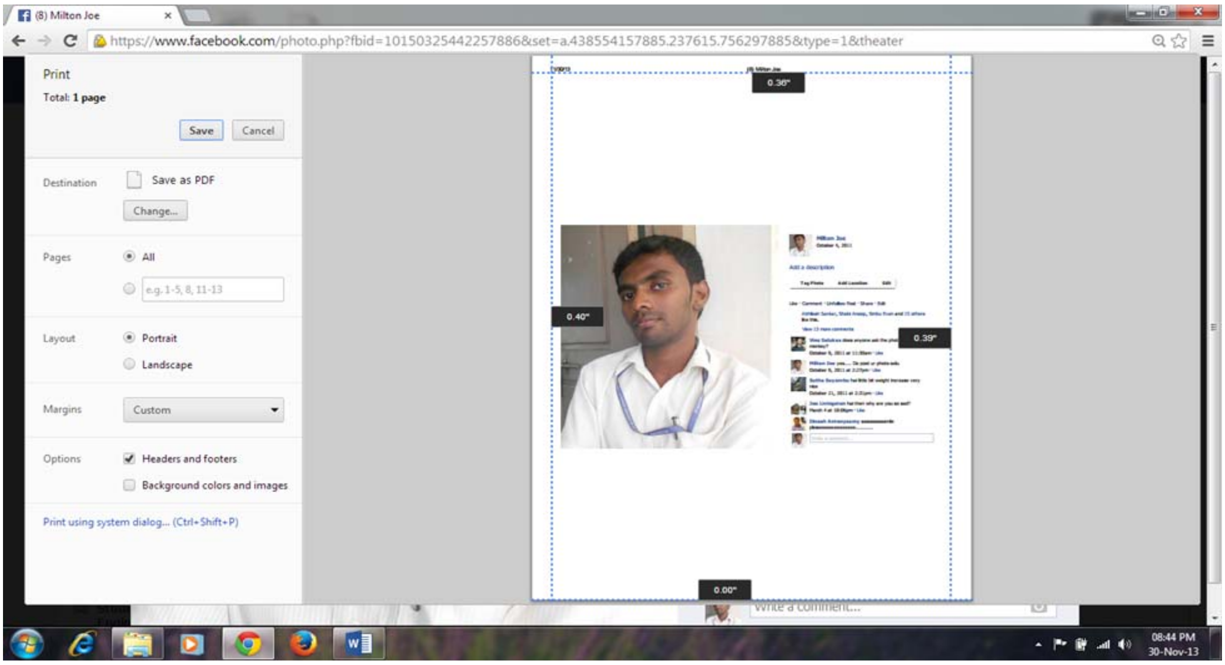

Milton Joe
https://www.facebook.com/photo.php?fbid=10150325442257886&set=a.438554157885.237615.756297885&type=1&theater
Milton Joe
October 4, 2011
Add a description
Tag Photo
Add Location
Edit
Untitled - Notepad
File Edit Format View Help
5:56 PM
12/24/2013

Figure 6 Screenshot of the web page by keeping another working environment as active window

F. Print Preview and Save


(8) Milton Joe
https://www.facebook.com/photo.php?fbid=10150325442257886&set=a.438554157885.237615.756297885&type=1&theater
0.36"
0.40"
0.39"
0.00"
08:44 PM
30-Nov-13

Print
Total: **1 page**
Save Cancel

Destination: Save as PDF (Change...)

Pages: ● All ○ e.g. 1-5, 8, 11-13

Layout: ● Portrait ○ Landscape

Margins: Custom

Options: ☑ Headers and footers ☐ Background colors and images

Print using system dialog... (Ctrl+Shift+P)

Figure 6 Print Preview and save the image in social networking webpage

Print preview option enables users to view the document's appearance before it is being printed. This option allows users to save the print preview appearance of the document to the computer system as pdf file. In the same way, this option can be used in the social networking websites to save the webpage as the pdf file. Similarly the webpage that contains user's photo can be saved using the print preview option. After saving the file to the computer system, then the image alone can be cropped and can be misused. In order protect the user data in the social networking websites, this print preview and then save option must be disabled. For the same, this paper proposes the same identifier key matching, which is used in the Print Screen option section. That is when the print preview option is chosen, it must check the identifier. If the identifier is equal to 111 then print preview of the current webpage is displayed but the save option must be disabled. If the identifier is not equal to 111, then normal operation of print preview can be used.

The Figure 6 represents the working process of Print Preview option in online social networking webpages. As shown in the image, left top corner we can find the save option, which enables the user to save the page as the pdf file. This form of image hacking can be eliminated in the propose model.

G. Temporary Internet Folder

Every browser keeps a folder in the local drive called temporary internet folder, which is used to store the caches. When a web page is loaded, the browser keeps the copy of the content of the web page in the temporary internet folder. This helps a lot, when the user loads the same web page again in future. That is, the content of the web page is directly loaded from the temporary internet folder, while downloading the new contents alone from the web server. The mechanism of caching provides the fast loading of the web pages in the client machine. As the name implies it is not really temporary internet folder. As long as the user clears the temporary internet folder manually, all the contents remain inside the folder. This temporary internet folder leads to privacy issue. Temporary internet folder can be opened easily by anyone, who has access to the machine and can copy all the images and other details.

In our case, when the hackers load online social networking web page in their local machine, all the images are stored in temporary internet folder. Once the images are downloaded to the hacker's local machine, those images can be used as hacker wishes. The ultimate aim of this paper is prevent the image hacking in online social networking web pages. The caching of web pages provide fast loading and viewing of the websites in client machine. In order to prevent the data hacking, this paper proposes an alternative method of storing caches of web pages. Temporary internet folder should contain a sub folder and it should be highly secured. This sub folder should not be open access, so that the user cannot open the secured sub folder. As discussed in the previous section all the social networking websites are alerted with the same identifier that is 111. When the user loads a website, the browser must check the identifier of the website. If the identifier is equal to 111, the content of the website must be cached to the sub folder. If the identifier is not equal to 111, then the content can be stored in the normal temporary internet folder. Once the content of the social networking websites are stored in the secured sub folder the images cannot be hacked by the hackers, since the sub folder cannot be opened by the user.

V . Conclusion

In this paper, the entire characteristics of Online Social Networking websites are studied and found the present security mechanism to the user data especially to user's photographs are not trust worthy. The user's photographs can be hacked in various ways. This limitation must be avoided to provide good quality of service to the users of Online Social Networking websites. This paper identified the various ways of hacking the user data in social networking websites and novel alternative mechanisms are presented to tighten the security constraints in Online Social Networking websites. The proposed methodologies are applicable only to the social networking websites, however if needed the same techniques can be implemented in other webpages also. Modeling of this paper makes sure, that security constraints of social networking websites are enhanced. Proposed architecture provides much better Quality of Service to all the users of Online Social Networking websites. The proposed methodologies and ideas are in the hand of operating system developers and the browser developers. The developers of both must consider the above mentioned factors, and develop their product accordingly to enhancing the security constraints in social networking websites.

References

[1] M. Milton Joe, Dr. B. Ramakrishnan, Dr. R.S. Shaji "Prevention of Losing User Account by Enhancing Security Module: A Facebook Case", Journal of Emerging Technologies in Web Intelligence, Vol. 5, No. 3, August 2013, Page No: 247-256.

[2] http://en.wikipedia.org/wiki/Social_networking_service

[3] 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.

[4] Facebook, Facebook Statistics, March 2011. <http://www.Facebook.com/press>.

[5] Twitter, Twitter Numbers, March 2011. <http://blog.twitter.com/2011/03/numbers.html>.

[6] Facebook, http://en.wikipedia.org/wiki/Facebook

[7] www.socialnetworkingwatch.com/all_social_networking_statistics/

[8] 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.

[9] Fatemeh Raji, Ali Miri, Mohammad Davarpanah Jazi, "CP2: Cryptographic privacy protection framework for online social networks", Computers and Electrical Engineering – Volume 39, issue 7, October 2013, Pages: - 2282 – 2298.

[10] Lucas MM, Borisov N. FlyByNight: mitigating the privacy risks of social networking. In: 7th ACM workshop on privacy in the electronic society (WPES'08); 2008. p. 1–8.

[11] Luo W, Xie Q, Hengartner U. FaceCloak: an architecture for user privacy on social networking sites. In: IEEE international conference on privacy, security, risk and trust (PASSAT-09). Vancouver, Canada; 2009. p. 26–33.

[12] Guha S, Tang K, Francis P. NOYB: privacy in online social networks. In: First workshop on online social networks (WOSP'08); 2008. p. 210–30.

[13] Baden R, Bender A, Spring N, Bhattacharjee B, Starin D. Persona: an online social network with user defined privacy, and scholarship. In: Annual conference on special interest group on data communications (ACM SIGCOMM); 2009. p. 135–46.

[14] Tootoonchian A, Gollu KK, Saroiu S, Ganjali Y, Wolman A. Lockr: social access control for web 2.0. In: The first ACM SIGCOMM workshop on online social networks (WOSN). Seattle, WA; 2008. p. 43–8.

[15] Tootoonchian A, Saroiu S, Ganjali Y, Wolman A. Lockr: better privacy for social networks. In: The 5th ACM international conference on emerging networking experiments and technologies (CoNEXT). Rome, Italy; 2009. p. 169–80.

[16] Yazan Boshmaf, Ildar Muslukhov, Konstantin Beznosov, Matei Ripeanu, “Design and analysis of a social botnet”, Computer Networks 57 (2013) 556–578.

[17] M. Milton Joe, R.S. Shaji, F. Ramesh Dhanaseelan “Detection of M-Worm to Provide Secure Computing In Social Networks” Elixir International Journal – September -50 (2012) 10363-10365.

[18] Wei Yu, Xun Wang, Prasad Calyam, Dong Xuan and Wei Zhao, “Modeling and Detection of Camouflaging Worm”, IEEE Transactions on Dependable and Secure Computing, Vol.8, No.3, May-June 2011.

Mr. M. Milton Joe received his B.Sc Computer Science degree from Bharathidasan University, India and MCA degree from Anna University, India. Presently he is working as Assistant Professor at St. Jerome’s College in Nagercoil, India. He has three years of research experience and authored nine research papers in reputed international journals. His research interests include Web Security, Web Communication, Vehicular Network and Social Network Security.

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. He has twelve years of research experience and published more than twenty five international journals. His research interests lie in the field of Vehicular networks, mobile network and communication, Cloud computing, Green computing, Ad-hoc networks and Network security.