IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-6, Issue-6, Jun 2018 E-ISSN: 2347-2693

Data Exposure Check & A Comprehensive Login Procedure

Poonam Dabas[1], Sheeba Sharma[2*]

[1] Dept. of CSE, University Institute of Engineering & Technology, Kurukshetra University, Kurukshetra, Haryana, India
[2] Dept. of CSE, University Institute of Engineering & Technology, Kurukshetra University, Kurukshetra, Haryana, India

[*]*Corresponding Author: sheebasharma10@gmail.com*

Available online at: www.ijcseonline.org

Accepted:11/Jun/2018, Published: 30/Jun/2018

***Abstract*—** A Social Network is a network which comprises countless interactions among people whether they are personal or professional. Social networks provide us with a platform to interconnect with each other through text or media in the name of messages, comments, pictures, posts, tags etc. Nowadays, the number of social networks in on an exponential rise, Facebook and Twitter etc. being the renowned ones. Social networks are vast networks which store and maintain information with respect to each user in their databases. That information is mostly contributed by the users only. That contribution being a voluntary one or an uneducated one is entirely another matter. This was the first key motive for our research. Enforcing a secure and comprehensive login process to secure the access of social accounts was the second one. In this paper, we propose a tool to evaluate the vulnerability of Facebook accounts w.r.t the privacy options provided by the social network. We also propose a reinvented login process with an aim to eradicate the perils of unauthorized access to the accounts.

***Keywords*—** Social networks, SNS, Privacy, Data-exposure, Privacy check, Login Process, Reinvented, Social Vulnerability

I. INTRODUCTION

Social networking sites are a majestic platform which not only empowers us to stay in touch with our friends and colleagues but also offers us an opportunity to build new relations. Facebook, LinkedIn, Twitter, Instagram and Snapchat etc are the prime examples of social networks. Like any other technology, social networks come with reservations as well. They may be providing us with the best features but at what cost? Our privacy? With the features, they also have the responsibility to keep our data safe and secure from malicious parties as well as provide us with ample privacy settings so that we can choose who can have access to that data. In this paper, we won't be stressing on new privacy options but the ones which are already being provided by one of the finest social networks i.e. Facebook. Nowadays, Social networks have come a long way and provide us with so much privacy options w.r.t. every single detail we save on it that most people aren't even aware of the options. They don't even know the power they have with respect to their own data, let along how to exercise it [1, 2]. Everything has a downside, which is why we often need to maintain a balance between things. If we choose the stringent privacy options for everything then we won't be able to utilize the social network at all while if we set all privacy options to the wobbliest ones, then we would be advertising even our confidential information.

In this paper, First we propose a tool to check our data exposure with respect to every single profile, so that the users can be advised about the vulnerability of their profiles and then we recommend privacy options which keep the balance to achieve a decent level of privacy while still being able to get the most out of social network [3]. In the second part, we propose a reinvented login process to secure the account access by making it more convenient and eradicating any loopholes the adversaries may exploit.

II. DATA EXPOSURE CHECK FOR FACEBOOK

Every social network requires its users to enter a variety of details in order to create a user profile. Such information may range from trivial to crucial which is why we need to set different levels of privacy for all those details. The option to set a different level of privacy for everything provides us with enormous power over our data. These settings may depend on the user's requirements as well as the user's personal wishes. Most of the users on social networks aren't even aware of the privacy options they are provided by the social networks [2, 4, 5]. Our proposed tool is for implementation by Facebook itself rather than any user because of it being more efficient and successful on Facebook's end. In this tool, we consider all the choices provided by Facebook and assess those choices based on our proposed system, while providing the user with his/her data exposure level in a numeric form.

Profile Details	Privacy Settings	Points	Recommended	Maximum Score
Address	Public	0		
	Friends	5		
	Custom	7		
	Only Me	15	✓	✓
Social Links	Public	0		
	Friends	2		
	Custom	3	✓	
	Only Me	5		✓
Websites	Public	0		
	Friends	2		
	Custom	3	✓	
	Only Me	4		✓
Emails	Public	0		
	Friends	5		
	Custom	7		
	Only Me	15	✓	✓
Phone Numbers	Public	0		
	Friends	5		
	Custom	7		
	Only Me	15	✓	✓
Timeline Visibility	Public	0		
	Friends of Friends	3		
	Friends	5	✓	✓
Birth Day	Public	0		
	Friends	5	✓	
	Custom	7		
	Only Me	10		✓
Birth Year	Public	0		
	Friends	6		
	Custom	8		
	Only Me	13	✓	✓
Interested In	Public	0		
	Friends	2		
	Custom	3	✓	
	Only Me	4		✓
Languages	Public	0		
	Friends	1	✓	
	Custom	2		
	Only Me	3		✓
Religious Views	Public	0		
	Friends	5		
	Custom	7	✓	
	Only Me	10		✓
Political Views	Public	0		
	Friends	5		
	Custom	7	✓	
	Only Me	10		✓
Relationship Status	Public	0		
	Friends	3		
	Custom	4	✓	
	Only Me	6		✓
Family Members	Public	0		
	Friends	1		
	Custom	2	✓	
	Only Me	4		✓
Life Events	Public	0		
	Friends	3		
	Custom	5		
	Only Me	8	✓	✓
About You	Public	0		
	Friends	4		
	Custom	6	✓	
	Only Me	10		✓
Friend Lists	Public	0		
	Friends	3		
	Custom	5		
	Only Me	15	✓	✓
Likes (Movies, TV Shows etc)	Public	0		
	Friends	3		
	Custom	4	✓	
	Only Me	7		✓
Favourite Quotes	Public	0		
	Friends	2		
	Custom	3	✓	
	Only Me	4		✓
Work	Public	0		
	Friends	5		
	Custom	7	✓	
	Only Me	10		✓
Education	Public	0		
	Friends	5		
	Custom	7	✓	
	Only Me	10		✓
Professional Skills	Public	0		
	Friends	2	✓	
	Custom	3		
	Only Me	5		✓
Hometown	Public	0		
	Friends	5		
	Custom	7		
	Only Me	15	✓	✓
Current City	Public	0		
	Friends	3		
	Custom	4	✓	
	Only Me	7		✓
Search Engines Profile Access	On	0		
	Off	15	✓	✓
Profile Picture	Public	0		
	Friends of Friends	3		
	Friends	5	✓	
	Custom	7		
	Only Me	10		✓
Albums	Public	0		
	Friends of Friends	3		
	Friends	5		
	Custom	6	✓	
	Only Me	10		✓
Future Posts Visibility	Public	0		
	Friends	4		
	Custom	6	✓	
	Only Me	9		✓
Past Posts Visibility	Public	0		
	Friends of Friends	3		
	Friends	7	✓	
	Custom	8		
	Only Me	9		✓
People, Pages, lists you follow	Public	0		
	Friends	3	✓	
	Custom	4		
	Only Me	7		✓
Friend Requests	Public	0		
	Friends of Friends	5	✓	✓
Email Lookup	Public	0		
	Friends of Friends	3		
	Friends	7	✓	✓
Mobile Number Lookup	Public	0		
	Friends of Friends	4		
	Friends	8	✓	✓
Public Key (PGP)	Public	0		
	Friends	7		
	Custom	10	✓	✓
Total			241	300

Figure 1- Parameters considered for assessing the Data Exposure on Facebook

Facebook provides us with the following options for every type of data:

1. *Public*

   In this option, the information is available to all the public available on Facebook with no restrictions whatsoever. It is the weakest option when it comes to data exposure [6, 7, 8].
2. *Friends*

   In this option, a user can set information to be visible to people only in his/her friend list which he/she has himself/herself added/accepted [6].
3. *Custom*

   This is the most flexible option with maximum customization. In this option, the user gets to choose specific friends he/she wants to share the information with. He/she can even form groups for the same.
4. *Friends of Friends*

   In this option, the friends of user's approved friends also have access to the information we set this option for.
5. *Only Me*

   Only Me means that no one except the user can access this information. This is the most stringent privacy setting but also acts as a bottleneck with respect to the usage of Facebook.

In our system, we have analyzed every single privacy option provided by Facebook by allotting a score for every such option. The numeric score counterpart of every user chosen option is added to the Data Exposure value with the most stringent options having a high score while the weakest choice having a low score. Our system assesses all the privacy options set by the user and adds the privacy score for such choice. Facebook provides us with privacy settings for 34 such types of information and lets us customize according to our own convenience.

For Example, if we consider a user's address then Facebook provides the user with four options being 'Public', 'Friends', 'Custom' and 'Only Me'. In our system, we have assigned 0 score for 'Public' option since it is the weakest setting while allotting 5 points to the 'Friends' option, 7 points for 'Custom' option and 15 points for the 'Only Me' option due to it being the stringent one. We recommend this setting to be kept 'Only Me' since a user's address is something that acts as a bridge between his/her online social network and real life. If unsolicited malicious parties get access to this data, the user may be vulnerable to threats like stalking and personal danger in his/ her real life. [2, 9, 10]

Similarly, we assign scores to the privacy settings set for the political and religious views of the user due to the sensitive nature of that information. This information can cause havoc for the user if subjected to the wrong audience. In another example, the ability of search engines to index the user's profile when searched publicly also affects the data exposure score of the user profile as it acts as an ingress from the cyber world outside of the actual domain. [11, 3, 12]

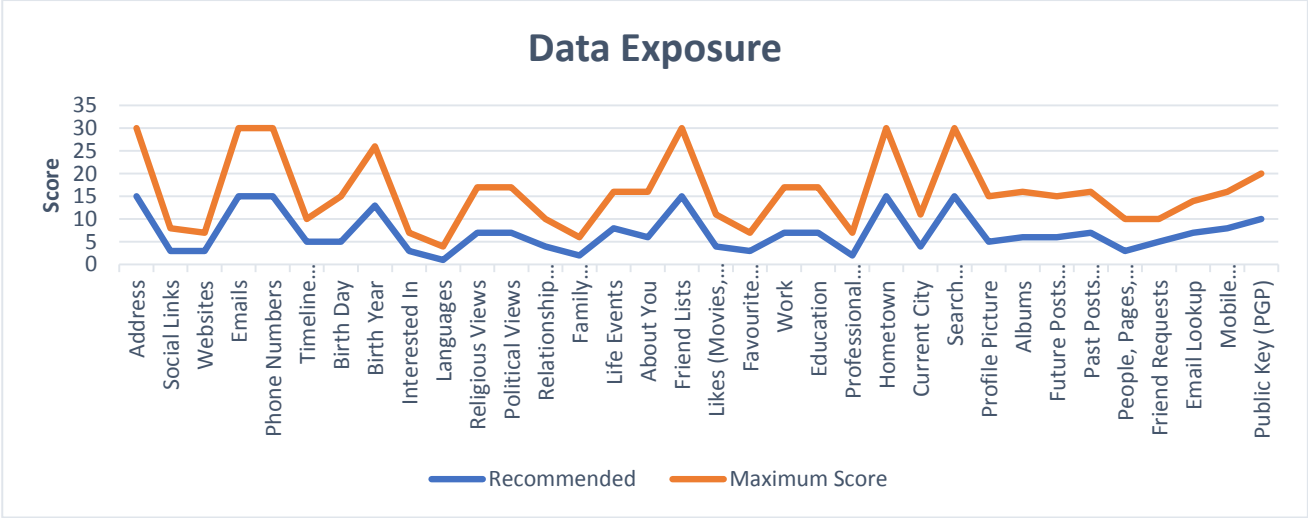

Figure 2- Threshold value vs Maximum Value

In our system, the same procedure is engaged for every such option and a final privacy exposure score is subtracted from the maximum privacy score while calculating the percentage exposure for every account. After choosing the options recommended by us, we found 19.666 % exposure to be the perfect balance between privacy and social network's appropriate usage. With 19.666% exposure, a user can utilize the services provided by Facebook while also keeping the information safe.

III. COMPREHENSIVE SECURE LOGIN PROCESS

Apart from the privacy settings, the one thing that matters more is security. No matter how tight and comprehensive our privacy settings are, they are of no use if we have a network or login process prone to infiltration. The login process needs to be a blend or security as well as convenience. We must not need to compromise with the security of the process for convenience or vice versa.

In our proposed login procedure, we propose an amalgamation of various modules which provide a successful noble equilibrium of protection and expediency.

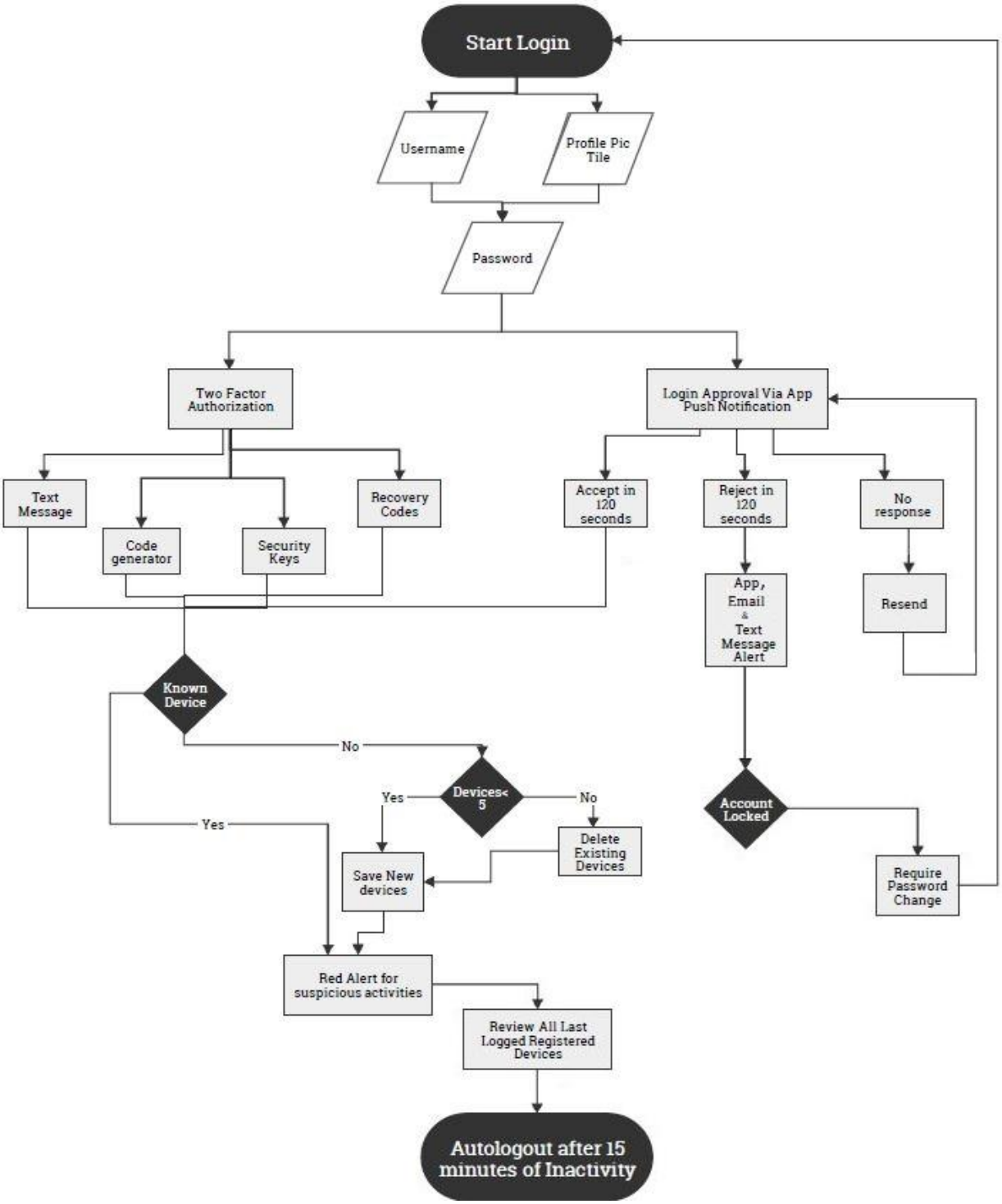

Figure 3- Proposed Login Process

1. *Two Factor Authentication Code*

The need for an extra code apart from the username and password is referred to as two-factor authentication. Two-factor authentication is already available in various social networks, but the delivery mechanism of codes varies. In our approach, the following methods have been adopted. [13, 14, 15]

a. *Text Message* – In this delivery mechanism, the code is delivered via a text message to the user's mobile phone. That code can be used to access the user's account along with the password for the account in question. The problem with this option is that it depends on the telecom operators, which may cause a delay in the delivery of the said code, rendering it useless.

b. *Code Generator* – The most widespread way for delivery of the code is the authenticator app. It works by adding a one-time key to the authenticator app, which then provides us with a code for login purpose. That code changes every 1 minute and is based on the accurate time from an NTP server and the key provided by the social network. There may be issues with the code if the time isn't in perfect sync with the NTP server. [14, 13]

c. *Security Keys* – In this code distribution mechanism, the user is provided with pre-set security keys to be used while logging in. Such security keys may be software or hardware. Social networks may require us to plug in a USB device which holds the security key.

d. *Recovery Codes* - These are the codes which are delivered to the user while setting up the two-factor authentication. These codes are to be used in emergency scenarios when the user doesn't have access to the usual delivery mechanisms. [14]

2. *App Push Approval*

In this module, the user gets a notification on his/her phone when logging into his/her account. The user is allotted 120 seconds time to respond to the notification with an acceptance or rejection. If the user accepts the request within 120 seconds, it takes the user to the next step of the login process. In case, the user rejects the request in 120 seconds then, he/she gets a detailed notification of the unauthorized attempted login via app email as well as text message. In such a scenario, the account gets locked and requires the password to be changed before next login. In the event that the user doesn't respond to the notification and neither accepts nor rejects that request, the notification expires in 120 seconds and is sent again after confirmation.

3. *Known Devices*

This module is encountered after a successful login. The account can remember only 5 trusted devices at a time. After the login process, the social network first checks if the device is enrolled as a trusted device. In case it is not enrolled, the social network asks the user to add it to the list of trusted devices in order to access the account. In a scenario, where the account already has 5 trusted devices, the system asks the user to replace an existing trusted device. After successful confirmation, the social network opens a popup showing any suspicious activities on the account and then shows another popup with a list of registered devices.

4. *Auto Logout*

In a situation, where the account stays inactive for more than 15 minutes, the account asks for the password again to remain active whenever accessed.

IV. METHODOLOGY

The method we proposed for obtaining the data Exposure of Facebook accounts is intended to be employed on Facebook's end, to be made available for every user's account since the parameters used are private to the user and Facebook only. One more reason for this is that the process of attaining the data exposure value as well as the value itself needs to be kept confidential as it is meant for the users' only. The approach has been implemented with the help of Python and its Data Analysis Library.

Technologies Employed

For the implementation of our system, we used Python 3.6 with the specialization of Python Pandas- The Python Data Analysis Library with the minor aid of Facebook graph API. Python Data Analysis Library is an optimum option for text processing, data extraction as well as data analysis. [16]

The dataset we fabricated in the implementation was tailor-made for our research purpose. Datasets were hard to find owing to the latest changes in social networks' terms and conditions. A plethora of old datasets was available, but they turned out to be immaterial, outdated and huge. For the purpose of our concept, we had to use the Facebook Graph API with many details fabricated and added to the dataset.

V. CONCLUSION AND FUTURE SCOPE

Online Social Networks(OSNs) have become an indispensable part of everybody's being and like any other technology, it has its downsides and vulnerabilities as well. The reinvented login procedure we proposed, covers each and every vulnerability and delivers as much convenience as possible. The subsequent proposal we made was custom-made for Facebook and accomplishes transparency and edification. It informs the users about the frailties in their privacy settings and the level of data exposure they are facing. The main purpose of our second proposal which we efficaciously accomplished was to apprise users about the control they have over their own data and its privacy.

REFERENCES

[1] A. Acquisti and R. Gross, "Imagined communities: Awareness, information sharing, and privacy on the Facebook," in *International workshop on privacy enhancing technologies*, 2006.

[2] B. Debatin, J. P. Lovejoy, A.-K. Horn and B. N. Hughes, "Facebook and online privacy: Attitudes, behaviors, and unintended consequences," *Journal of Computer-Mediated Communication*, vol. 15, pp. 83-108, 2009.

[3] R. Gross and A. Acquisti, "Information revelation and privacy in online social networks," in *Proceedings of the 2005 ACM workshop on Privacy in the electronic society*, 2005.

[4] A. Hannak, P. Sapiezynski, A. Molavi Kakhki, B. Krishnamurthy, D. Lazer, A. Mislove and C. Wilson, "Measuring personalization of web search," in *Proceedings of the 22nd international conference on World Wide Web*, 2013.

[5] H. R. Lipford, A. Besmer and J. Watson, "Understanding Privacy Settings in Facebook with an Audience View.," *UPSEC*, vol. 8, pp. 1-8, 2008.

[6] F. Stutzman and J. Kramer-Duffield, "Friends only: examining a privacy-enhancing behavior in facebook," in *Proceedings of the SIGCHI conference on human factors in computing systems*, 2010.

[7] V. Toubiana, A. Narayanan, D. Boneh, H. Nissenbaum and S. Barocas, "Adnostic: Privacy preserving targeted advertising," 2010.

[8] A. Korolova, "Protecting privacy when mining and sharing user data," 2012.

[9] Y. Liu, K. P. Gummadi, B. Krishnamurthy and A. Mislove, "Analyzing facebook privacy settings: user expectations vs. reality," in *Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference*, 2011.

[10] K. Raynes-Goldie, "Aliases, creeping, and wall cleaning: Understanding privacy in the age of Facebook," *First Monday*, vol. 15, 2010.

[11] C. Castelluccia, E. De Cristofaro and D. Perito, "Private information disclosure from web searches," in *International Symposium on Privacy Enhancing Technologies Symposium*, 2010.

[12] N. Wang, H. Xu and J. Grossklags, "Third-party apps on Facebook: privacy and the illusion of control," in *Proceedings of the 5th ACM symposium on computer human interaction for management of information technology*, 2011.

[13] F. Aloul, S. Zahidi and W. El-Hajj, "Two factor authentication using mobile phones," in *Computer Systems and Applications, 2009. AICCSA 2009. IEEE/ACS International Conference on*, 2009.

[14] C. F. Austin, X. Wan and A. Wright, *Two-factor authentication*, Google Patents, 2014.

[15] A. T. B. Jin, D. N. C. Ling and A. Goh, "Biohashing: two factor authentication featuring fingerprint data and tokenised random number," *Pattern recognition*, vol. 37, pp. 2245-2255, 2004.

[16] W. McKinney and P. D. Team, "Pandas—Powerful Python Data Analysis Toolkit," *Pandas—Powerful Python Data Analysis Toolkit*, p. 1625, 2015.

[17] C. Dwyer, S. Hiltz and K. Passerini, "Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace," *AMCIS 2007 proceedings*, p. 339, 2007.

[18] U. Maheswari and S. Balaji, "Privacy Preservation on Online Social Networking Issues and Challenges," *International Journal of Computer Sciences and Engineering*, vol. 5, no. 8, pp. 215-217, 2017.

[19] B. Kasab, S. Ubale and V. Pottigar, "Enabling Privacy Preservation Technique to Protect Sensitive Data with Access Control Mechanism Using Anonymity," *International Journal of Computer Sciences and Engineering*, vol. 3, no. 10, pp. 61-65, 2015.

Authors Profile

Mrs. Poonam Dabas is currently working as an Assistant Professor in the Department of Computer Science and Engineering, University Institute of Engineering and Technology, Kurukshetra University, Kurukshetra and has teaching experience of more than 12 years.

Ms Sheeba Sharma is currently pursuing Masters of Technology from University Institute of Engineering and Technology, Kurukshetra University, Kurukshetra and completed her Bachelors of Technology from Kurukshetra University in 2016.

