IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Volume-5, Issue-8 E-ISSN: 2347-2693

Privacy Preservation on Online Social Networking Issues and Challenges

Uma Maheswari[1*], S. Balaji [2]

[1*]Dept. of Computer science, D.B.Jain College, Chennai, India
[2]Dept. of Computer science, D.B.Jain College, Chennai, India

**Corresponding Author: haree_sow@gmail.com,*

Available online at: www.ijcseonline.org

Received: 02/Jul/2017, Revised: 14/Jul/2017, Accepted: 10/Aug/2017, Published: 30/Aug/2017

***Abstract*-**Over the past few years, the popularity of social networking sites (SNS) has increased immensely. In the internet age, these social networking sites like Facebook, Twitter, Orkut, LinkedIn, MySpace, etc not only offer the scope of connecting also offers the scope of getting updates at any possible hour of the day. Online networks provide significant advantages both to the individuals and in business sectors. Many users provide information about themselves on social network which can be searched and hacked by the strangers. Thus, it raises privacy and security issues. Unfortunately many users are not aware of this.This paper elaborates Privacy issues concerned with social networking and proposes a framework to deal with. In this paper, study is made on how the current privacy plays on social network sites, how personal information is being influenced by internet and social network, and also how the privacy become a risk and how to employ security awareness to avoid privacy risk.

Keywords :-Social Networking, Privacy, Security, Internet, Hacking.

I. INTRODUCTION

Over the past few years, the popularity of social networking sites (SNS) has increased immensely. In the internet age, these social networking sites like Facebook, Twitter, Orkut, LinkedIn, MySpace, etc not only offer the scope of connecting also offers the scope of getting updates at any possible hour of the day. What is more interesting is that only a little knowledge about how these sites work is enough to start. The least that a user has to do is to create a profile and get started. The basic objective of using the social networking sites is online communication and interaction. For using the social networking sites, the users need to make an online profile through which they can share information and messages with their friends. Mostly the sites encourage the users to start the account or to create the profile using real names and information as they offer various privacy measures where the personal information is not disclosed. Mostly the young people aged between 15 to 25 years use the popular social networking sites regularly. For them networking socially means Facebook, Twitter, Myspace and the like. The world to them basically means the internet and the social networking sites where they can get connected to friends (existing as well as new ones. There are both positive and negative sides of social networking sites. The online virtual world, where even small information about almost anything is available at every possible time of the day, the young technology savvy generation does not really seem to care about the online privacy threats[1]. Section I contains Introduction to impact of Online social networking. Section II analyses related work on privacy issues in social networking. Section III concerned with Privacy problem. Section IV discusses the Privacy framework and trust model.Section V concludes with the privacy concerns of social networking.

II. BACKGROUND WORK

Social networking sites and associated privacy concerns is one of the most debated topic nowadays as participation in such sites has increased dramatically. A number of journals and articles come up with this issue that how the increase in the usage of social networking sites is leading to various online crimes.

A blog in a website DashBurst clearly mentions that “with the rise of social media, privacy concerns have taken a backseat in recent years ”. It talks about the potential dangers that a young user may likely face while using the social networking site. Thus it becomes very important for one to read the privacy policies and measures offered by these sites in order to have a safe online networking. Further, the blog also states the privacy policy changes brought out by the popular sites like Facebook and Twitter and how it has affected the users[2].

V. Raghunatha Reddy and C.V. Madhusudan Redd work proposed the system will check the user’s existence in the database and provide the set of services with respect to the role of the user.

The application is based on three-tier architecture. The cipher key will be used to find the fraud application. This approach is called Anti-Phishing. Anti-Phishing is nothing but “preventing the phishing” With the controversial changes made by the popular social networking site Facebook in 2009, it had beome quite impossible to maintain a safe invisible account. By analysing the personal information revelation behaviour of the users, it has been mainly found out that this factor mainly revolves around hobbies and interests although it also has other directions. Like for insance, semi-public information may include schooling or employment details, whereas personal information may include drinking or drug habits or sexual orientation, etc[3].

Johnson et al. recruited 260 Facebook users to install a Facebook application that surveyed the users’ privacy concerns, their network compositions, the sensitivity of the posted content and their privacy preserving strategies. Their study showed that 86.2% of participants were unconcerned with the threats of strangers viewing their profile content.
They could figure out that the threats from inside the network were more of a concern to the users. One drawback with their work was that the sample used in their work was biased toward users who were unconcerned with privacy.
W. Binden work looked at the association between network compositions, expectancy violation and interpersonal privacy practices of having a friends only profile. They drew Petronio’s theory of communications privacy management (CPM) which discusses iterative process of rule development. It regulates who to tell what and boundary coordination which develops disclosure ownerships and permeability rules in the network.

III. PRIVACY PROBLEM

Three different privacy problems are defined and tackle. Those are Social privacy problem, surveillance privacy problem and institutional privacy problem[4].

A. Social Privacy Problem

Social privacy concerns describe people’s fear of intrusion caused by other people. They capture for example the fear of being stalked, bullied or being exposed to unpleasant content. An informal social gathering, especially one organized by the members of a particular club or group.
Some sites may share information such as email or user information with other parties.

Nowadays the Social Network service providers encourage non-users to participate and users to engage more and more. This is done by means of the site design (“what’s on your mind?”, “help XY find friends”, “write something”, “write a comment”…), the affordances of the technology and driven by Social Network sites very business model[5].

B. Institutional Privacy Problem

Suppose we click on some advertisement, our information is stored on the particular company so we can lose our information. peoples fear of intrusion caused by public or private institutions such as the use personal data for undesired purposes. Some private companies are decided to attract people so; those are intended to create prestige rather than immediate sales. In marketing the ‘collect once, use many times’ approach practiced in government organizations, agencies[6].

C. Surveillance privacy problem

Actually we don’t know who will see our profile/page/my friends. We don’t know who will retrieve our information. In present social networking sites we will retrieve some much of information about unknown persons also without telling him.

IV. MEASUREMENT THEORY

It is essential for an OSN user to understand the privacy risks that could follow after carelessly sharing the sensitive data online. In order to make the users aware of the data privacy concerns their information sharing behaviour along with the sharing behavior of their connections should be measured. Measuring this abstract and unobservable trait is a challenging task and is possible only if there is a proper metric of privacy[7].

Psychometrics is derived from the two words psycho and metrics which basically means ‘mental measurement’ . It is the subfield of psychology and is the science of measuring individuals’ unobservable characteristics. It involves the development and analysis of measurement instruments and theoretical approaches. Human beings either make a relative or an absolute judgment while comparing things.

A .Privacy framework

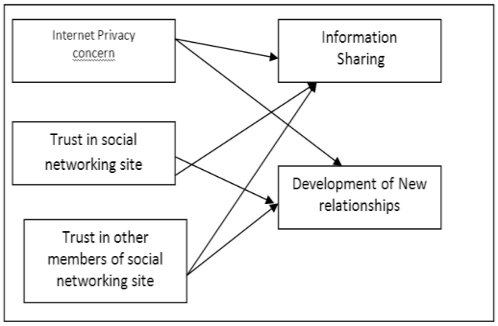
The main question is how interactions of users determine tie strength and implement privacy in online social networks[8]. More specically, we want to explore whether a user's interaction with his friends can be used as a basis for making data access decision for that user. To answer this question, we need to understand nature of privacy in online social networks and dynamics of interactions intensity for OSN users. We break main research question into three sub questions:

1. How to measure privacy risk associated with social graph of OSN users?
2. How to construct interaction graph by quantifying users interactions in OSN?
3. How to segregate audience on the basis of interaction graph in OSN?

From our first research question, It quantify the privacy risk attributed to friend relationship in online social networks.

We show that risky friends can reveal user personal information unintentionally in online social networks.

Second research question deals with user's interaction patterns in online social networks. It shows that users tend to interact mostly with small subset of friends, often having no interactions with majority of their friends in online social networks. This cast doubts on the practice of extracting meaningful relationships from social graphs. It suggest interaction based model for validating user relationships in online social networks. Third research question deals with audience segregation. The diagram 4.1 shows the inter-relationship between privacy and trust.


Internet Privacy concern
Information Sharing
Trust in social networking site
Development of New relationships
Trust in other members of social networking site

4.1 Privacy Trust Model

While people keep talking about privacy, the issue of the borderline between public area and private area of social media space are still unclear. In some situation, users want their personal information to be known only by a small circle of close friends, and not by strangers. While in other scenario, they are willing to reveal personal information to anonymous strangers, but not to those who know them better, like their father or mother.

V. CONCLUSION

The World Wide Web and the social networking sites are definitely opening up broader avenues of communication, at the same time; addiction to online social media is rising. Making friends with unknown people and increasing the numbers in 'friend list' in social networking sites might be considered as happening and trendy but can pose a tangible threat to one's privacy. Online world is abysmal and what is projected might not be real. Hence, when participating in the social networking sites the young users are required to be aware and vigilant.

REFERENCES

[1]. V. Raghunatha Reddy, C.V. Madhusudan Reddy, M. Ebenezar, "*A Study on Anti-Phishing Techniques"*, International Journal of Computer Sciences and Engineering,Volume-4 , Issue-1 , Page no. 30-36, Jan-2016

[2]. L. A. Cutillo and R. Molva , "*Safebook: A Privacy-Preserving Online Social Network Leveraging on Real-Life Trust*", IEEE, pp. 94-101, 2009.

[3]. A. Srivastava and G. Geethakumari, "*A Framework to Customize Privacy Settings of Online Social Network Users*," IEEE Recent Advances in Intelligent Computational Systems (RAICS), pp. 187-192, 2013.

[4]. A. Dhami, N. Agarwal, T. K. Chakraborty, B. P. Singh and J. Minj, "*Impact of trust, security and privacy concerns in social networking: An exploratory study to understand the pattern of information revelation in Facebook*," 3rd IEEE International Advance Computing Conference (IACC), pp. 465-469, 2013.

[5]. W. Binden, M. Jormae, Z. Zain and J. Ibrahim, "*Employing Information Security Awareness to Minimize Over-Exposure of Average Internet User on Social Networks,*" International Journal of Scientific and Research Publications, vol. 4, no. 1, pp. 1-6, 2014.

[6]. X. Chen and S. Shi, "*A Literature Review of Privacy Research on Social Network Sites*," International Conference on Multimedia Information Networking and Security, pp. 93-97, 2009.

[7]. F. Raji, A. Miri and M. D. Jazi, "*Preserving Privacy in Online Social Networks,"* Springer-Verlag Berlin Heidelberg 2012, pp. 1-13, 2012.

[8]. J. Ge, J. Peng and Z. Chen, "*Your Privacy Information are Leaking When You Surfing on the Social Networks: A Survey of the degree of online self-disclosure (DOSD),"* IEEE 13th Int'l Conf. on Cognitive Informatics & Cognitive Computing (ICCI*CC'14), pp. 329-336, 2014.

[9]. W. Binden, M. Jormae, Z. Zain and J. Ibrahim, *"Employing Information Security Awareness to Minimize Over-Exposure of Average Internet User on Social Networks,"* International Journal of Scientific and Research Publications, vol. 4, no. 1, pp. 1-6, 2014.

[10]. X. Chen and S. Shi, "*A Literature Review of Privacy Research on Social Network Sites*," International Conference on Multimedia Information Networking and Security, pp. 93-97, 2009.

[11]. F. Raji, A. Miri and M. D. Jazi, "*Preserving Privacy in Online Social Networks*," Springer-Verlag Berlin Heidelberg 2012, pp. 1-13, 2012.

[12]. J. Ge, J. Peng and Z. Chen, "*Your Privacy Information are Leaking When You Surfing on the Social Networks: A Survey of the degree of online self-disclosure (DOSD),"* IEEE 13th Int'l Conf. on Cognitive Informatics & Cognitive Computing (ICCI*CC'14), pp. 329-336, 2014.

[13]. Maritza Johnson, Serge Egelman, and Steven M Bellovin., *Facebook and privacy: it's complicated",* In Proceedings of the Eighth Symposium on Usable Privacy and Security, pp.9. ACM, 2012.

[14]. Abdullah Al Hasib., "*Threats of online social networks*", IJCSNS International Journal of Computer Science and Network Security,Vol.9, pp..288–93, 2009.

[15]. Balachander Krishnamurthy and Craig E Wills., "*Characterizing privacy in online social networks*", In Proceedings of the workshop on Online social networks, pp.37-42. ACM, 2008.

Authors Profile

Uma Maheswari. S, did Masters in computer science from Madras University. She has been serving teacher in a Primary school in Chennai. Her interests include Networking and security concepts.

Balaji. S. has been working as a faculty in the Department of Computer science over a decade. His interests include data structures and algorithms.