International Journal of Engineering &Technology, 7 (1.7) (2018) 142-145

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Privacy study on images uploaded in social networks

Hemalatha D[1]*, Almas Begum[2],Alex David S[3]

[1,2]Assistant Professor,[3]Associate ProfessorDepartment of Computer Science and Engineering, School of Computing,Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology,Avadi, Chennai-62, TamilNadu, India
**Corresponding author E-mail:hema24294@gmail.com*

Abstract

Presently, the growth of Social media is explosive among the users. Increasingly developed social websites like Flickr, Facebook, Google+, LinkedIn etc permits the users to create, share and view the post. Confidentiality is a leading factor required in Social Networks. The social users upload their photos to the social sites that intend to gain public interest for social purposes. The exposure of personal information leads to slipping process like identity stealing, morphing etc, which are against the privacy violations. Relied upon the personal characteristics of users, the privacy settings of each user should be defined. In this paper, a relational study about the privacy settings in Online Social structure is examined. Initiated by the importance of social networks among the social users and their behavior towards Online Social Networks, which is followed by the privacy techniques suggested by other researchers are explored. At last, an overview about the merits and demerits of privacy designs and schemes for the user-uploaded images are presented. The study results a new privacy system that controls the confidential information from being accessed from different devices, including mobile devices and computers.

Keywords: *Online Social Structure, Social Media Users, Privacy, Images, And Sensitive Information*

1. Introduction

With the advancements in the Online Social Networking, the growth of social media users is inclined. It assists the social users to make new contacts, old friends and sharing the common opinions with the group of people across the world. It acts as communication links among the users. As the increased usage of websites, the participation of user's rate is also increased. By this advent, the user's share their images and personal information to their communities. Without having prior knowledge about the privacy settings, the images are uploaded and shared among the group of people. By doing so, a variety of risks are faced by the social users like identity stealing, morphing etc. Despite these risks, many privacy mechanisms of content sharing sites are very weak.

A profile of a user comprised of details like company details, educational details, residential address, common interest etc. In order to be a part of the networks, tagging concept is emerged. An image of a user is tagged [1] with several people to gain interests. This concept becomes riskier in the complicated environment. And also, the users are unaware about the consequences of tagging concept of an image. Instead of imposing restrictions over such incidents or increasing security, sites like FB and Instagram are encouraging people to get into such things.

Online Social Networking is still in developing stage, but it elegantly supports some eminent applications [2]. As this technology grows, we, eventually, expect some advanced functionalities. It is not incredible that social structure will someday become de-facto portals for both personal and commercial online interactions. Users located adjacent in a social network tend to trust each other more than the users located in random pairs, which is shown in fig.1. Users browse neighbouring areas of their interpersonal organization as they need to discover important content. Witnessing how content direct these networks over a period of time and ends up prominently increasing important in commercial advertising, in political campaigning, and ultimately to society.

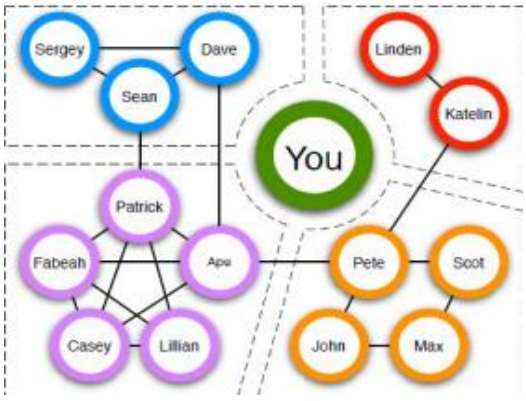


Fig.1. Community formation in Social networks

Further, paper is organized as follows: Section II discusses about the existing schemes suggested by other researchers and Section III discusses with summary of the review findings made in our study.

Copyright © 2018S Hemalatha D. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

2. Related Work

In this section, we present a clear idea about the significance of the Online Social Networks, User's behavior in Online Social Network (OSN) and techniques involved.

2.1 SIGNIFICANCE OF OSN

In depths of revolution in social media, it has become vital communication medium. The primary benefit of the social media is the sharing and gaining of knowledge from wide range of people. This kind of growth develops the communication skills towards the online learners. Social media has touched our lives, both on an interpersonal and a community level. These networks grow based on personal interactions over a time and connects users with the technological infrastructure, social know- how as well as technical expertise's.

2.2 USER BEHAVIOR IN ONLINE SOCIAL NETWORKS

The perception towards user behavior in Online Social Networks imposes a better interface design for improved content distributed systems. It is crucial to study about the behavior of users when they are associated to the social websites. Email is considered as important factor for associating with the networks [3]. In current scenario, the social links are interlinked with each other. A single account of user is associated with different social websites. It assists the service providers to identify the attitudes of users. In order to improve the user's experience, the behavior study is an important thing. In section 2.2, we explore the four orientations of defining the user behavior in social networks. The four orientations are as follows:

a)Finding the associations between users in OSN using Social Graph
b)Monitoring the events for predicting the network traffic
c)Development towards mobile platforms and applications
d)Security and privacy analysis-based user's behavior

a) Finding the associations between social users:

Social Graph is a mathematical model used for assessing the connections among the social users. It assists us to provide details about the characterization of user's behaviours. The table 1 depicts the knowledge of five eminent social networks.

Table 1. Knowledge about five eminent social networks [9]

SOCIAL SITES	NO. OF USERSIn billion
Facebook	1.01
Linkedin	200
Google +	450
Foursquare	30
Twitter	500

Social graph is modelled into two ways, namely, undirected graph model and directed graph model. The four fundamental graphs are listed in Table 2. Relied upon these sorts of graph, the associations among the OSN users are studied. In addition to this, it imposes to research about the efficacy of social graphs. To resolve this issue, the authors in [4], proposed crawling techniques.The friendship graph and interaction graph belong to the class of undirected graph and directed graph model includes latent graph and following graph. Friendship graph is defined that every user is considered as nodes and edge is represented as the connections between users. Therefore, friendship in OSNs can hardly be viewed the same as friendship in the real world. Interaction graph is defined to find the communication between the users in real- world entities. Then, the conventional measurement approaches are used for understanding the behaviors from browsing. Latent graph is built from the friendship graph and interaction graph. The overall system architecture is given in fig.2.

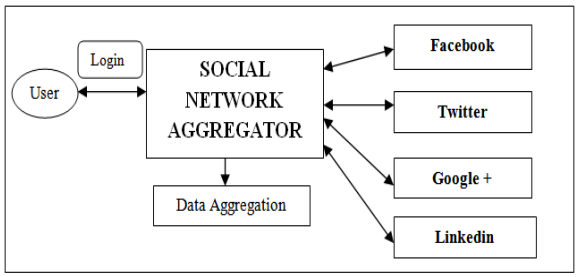


Fig.2. Profiling data through social network aggregator [11]

Table 2. List of different social graphs [12]

SORTS OF GRAPH	EDGE
Friendship Graph	Depicts the associations or connections between users
Interaction Graph	Depicts the posting behaviors
Latent graph	Depicts the browsing profile
Following graph	Depicts to obtain the messages

b)Network Monitoring analysis

A variant kind of social graphs intimates the associations between the users. In some cases, the user's activities can't be predicted due to restricted information about them. Internet service Provider has better understanding about traffic pattern between end user and social network sites and ability to provide optimized solution according to the OSN users. Instead of using crawling techniques, the network events also play a vital role to predict the user's behaviour. As in fig.2, Clickstream data is used for analysing the behaviour from Social Network Aggregator (SNA). Benevenuto et al studied about the user behaviour from Clickstream data analysis. The author in [5] collected user data for a week of time that intended to study about the behavioural aspects of social users.

Atlast, they concluded that the user's browsing data contain: i) Frequency of data access in OSN ii) Aggregate time spent on OSN iii) Session monitoring in OSNs. From their study, they encountered 40 types of user's activities with their traffic bytes [5]. And they also discussed about the user's transition using markov chain model. The study on behaviour of user in OSN is shared by Clickstream data. Due to restriction in usage and performance of data, it is incomplete. The features such as collection duration, behaviour of inactive user, monitoring location also limits the clickstream data.

c)Mobile Application Developments

Mobile platforms are also depicts the behavior of user. A variant number of web applications are emerged, so it is necessary to study about the mobile social networks. Some social websites also permits to access the data from mobile networks. In order to design mobile systems, the behavioral study of user is also important. By the advent of Bluetooth [6], the nearby users are recognized and the data is shared among them. This is referred as the social serendipity. For example, internal collaboration in companies can be sophisticated by serendipity for bringing the people working in the similar project together. The serendipity is fundamentally emphasized with privacy issues and tools related to it must be designed with care.

d)Anomalies Behavior

Due to the interlinkage of different social websites, there is a chance of exhibiting the threats. By the assistance of OSN service providers, user-user interaction is possible. The user may share their data like photos, articles, private messages etc. A Sybil attack is the most common threats found in the OSN. Some user's acts like original users and steal the account information. In [16], they presented the types of attacks, such as untrusted third-party applications, cross-site profile cloning, social spamming, and phishing prevails in OSN. In order to protect the sensitive information, decentralized OSN architecture is required.

2.3. IMAGE SHARING- PRIVACY ANALYSIS

Privacy is the most important parameter to be considered for web design. The association between privacy and user's network imposes a variety of privacy challenges. Nowadays, the images are being shared by most of the users. Sharing takes place both in group of people and in social circles. The sensitive information is mostly presented in the semantic enabled images. Relied upon the user's characteristic, the privacy setting of each user should be defined. In this section, we explore the privacy analysis towards user uploading the images. The need for automatic privacy settings is inadequate. In order to resolve this, several authors studied about the privacy suites for the uploaded images. The web applications developed by the software programmers are inadequate to provide automatic privacy settings. Internet privacy is the subset of data privacy. The large-scale computing systems involves large number of privacy settings.

Normally, the data privacy derives in two ways: a) Settings of self- privacy and b) Design of recommendation systems. The thought of issuing privacy to the users can be given for their uploaded data, profile information and associations and Meta data of the user uploaded images. Thus, the user uploaded images are classified into hierarchical structure, to define a priority set. Then, the concept of 'privacy by design' was introduced. Their purpose was to improve the applications design by including the privacyconcepts. Each application involves different level of privacy design with more authentic systems. The personal details of a user is shared by giving response to the received request was studied.

Table 3. Taxonomy of social networks (Rosenblum, 2007)

Region	Social websites
Africa	Hi5, Facebook
America(North)	MySpace, Facebook, YouTube, Flicker, Netlog
America (Central and South)	Orkut, Hi5, Facebook
Asia	Friendster, Orkut, Xianonei, Xing, Hi5, YouTube, Mixi
Europe	Badoo, Bedo, Hi5, Facebook, Xing, Skyrock, Ployaheod, Odnoklassniki.ru.V Kontakte
Middle East	Facebook
Pacific island	Bedo

In other words, privacy is characterized for self-representation of the online social networks i.e sharing their images and comment from others. In extending to privacy concern, [7] suggested a solution to its in three ways, namely, protective technologies, social awareness and legislative support. Protective technologies include authentication and access control mechanisms according to time. Then, creating knowledge about the privacy of the uploaded images is known as social awareness. Atlast, the shared images are enacted under the privacy law enforcement [7]. A general usage survey of facebook users was studied by [8]. They depicted that users share their 92% of profile pictures, 95% of data of birth, and 20% shows their contact details. And the similar study was conducted by [8] with information about the hacked users. The usage of internet services was mostly adopted by the youngsters. In reality, most of the young users are unaware about the privacy risks of sharing the images. Irrespective of the age, information sharing in the online environment causes dangerous to the social users. The confidence of the users is increased by the level of privacy settings. It should also be simple and easy to be used. The major risks faced by the users, identity theft i.e stealing the user's personal information like images, contact address etc). The different ways of stealing the user's information was analyzed by the [9].

Table. 4. Analysis of real identities (Gross and Acquisti, 2005)

Category	% of social users
Real name	90%
Partial name	4%
Fake name	6%

Some recent works investigated the self- configuring of the privacy settings. The privacy policies are preferred for the authorized users were studied by [10]. The communication was enabled among the authorized group of users. A machine learning models were used to obtain the data accord to its context was studied by [10]. This research study was further extended by forming clusters from partitioned users by [11]. Privilege based privacy settings was initiated by Ravindran et al, that predict user's privacy based on preferences. It was extended by [13], which assigns label to the selected group of users. His work enables to form privacy labels for unauthorized friends. The tagging concepts were improved by using access-control policies. The uploaded images contain keywords and labels for representing the images. A vast amount of study was conducted in Image Content Analysis [12].

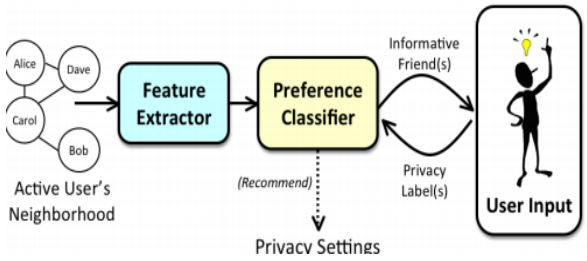


Fig. 2. Preferences based privacy settings [46]

A text-based image retrieval system was examined by [14]. They designed discriminative model that stores and retrieves the image based on the ranking system. The Latent Dirichlet Allocation (LDA) was proposed to align and arrange the image in an unsupervised fashion. Based on the topics, the images are represented. Then the semantic model was encouraged by [14]. They have additionally introduced the consequences of a broad test assessment, under different beforehand proposed test conventions, which exhibited better execution with deference than a sizable number of best in class techniques, for both semantic marking and recovery. In [15], examined another picture include called the shading correlogram and utilize it for picture ordering and examination. This component distils the spatial connection of huesand is both powerful and modest for content-based picture recovery. The correlogram vigorously endures huge changes fit as a fiddle caused by changes in review positions, camera zooms, and so forth.

Table 5. Example friend data with extracted features, including community-based features

	R_0	R_1	R_2	R_{20}	R_{21}	R_{22}	R_{23}	Privacy settings (Images)
Alice	0	1	0	0	0	0	0	Allow
Bob	0	0	1	1	0	0	0	Refuse
Carol	1	0	0	0	0	0	0	Allow

Table 6: Relational study of merits and demerits of privacy analysis

Techniques for privacy	Merits	Demerits
Design oriented privacy suites	Design policies are transparent in nature.	Difficult to understand by normal users
Study on social circles	Flexible for finding association among the users.	Unable to process for higher number of users.
Compression schemes for images	Simple to use	Overhead in computational process
Privacy protector tools	Transparent process	Highly difficult to understand
Tagging concepts	Transparent process	Inefficient handling of large set of users.
Linked data to the tags and keywords	Link with multiple sites	Limited set of connecting the linked data
Image classification and search for privacy schemes	Performs direct search for protected data	High complexity

3. Conclusion

Nowadays, a vast amount of private data is being shared in the social networking sites. The private data includes sensitive information and images, in which images are being mostly shared by most of the social users. In order to eliminate the malicious events, a well-reputed privacy schemes are required. But, in most of the cases, applying privacy schemes on the data is a cumbersome task. In this paper, relational study of privacy settings in Online Social Networks is examined. In specific to, we studied about the privacy settings for the user-uploaded images.

From this study, we summarized that the privacy oriented importance given to the user-uploaded images are not yet flourished. It is wisely recommended that a privacy design for user-uploaded images need to be developed. The privacy systems of Online Social Networks should accommodate their users with different levels of privacy settings for their images irrespective of location and time.

References

[1] White, T.; Chu, W.; Salehi-Abari, A.; "Media Monitoring Using Social Networks," Social Computing (Social Com), 2010 IEEE conferences on Social networking sites, 2010, pp.661-668.

[2] Rodrigues, E.M.; Milic-Frayling, N.; Fortuna, B.; "Social Tagging Behavior in Community-Driven Question Answering," Web Intelligence and Intelligent Agent Technology, 2008, pp.112-119.

[3] Nielsen Online Report, " Social networks & blogs now 4th most popular online activity", 2009.

[4] C. Wilson et al., "User Interactions in Social Networks and Their Implications," Proc. EuroSys, 2009.

[5] F. Benevenuto et al., "Characterizing User Behavior in Online Social Networks," Proc. IMC, 2009.

[6] F. Schneider et al., "Understanding Online Social Network Usage from a Network Perspective," Proc. IMC, 2009.

[7] Campisi, P.; Maiorana, E.; Neri, A., "Privacy protection in social media networks a dream that can come true?,", 16th International Conference on Digital Signal Processing, vol., no., pp.1,5, 2009

[8] Rosenblum, D., "What Anyone Can Know: The Privacy Risks of Social Networking Sites," Security & Privacy, IEEE,

[9] Novak, E. & Li, Q, "A Survey of Security and Privacy in Online Social Networks", College of William and Mary Computer Science Technical Report, WM-CS-2012-2

[10] J. Bonneau, J. Anderson, and L. Church. Privacy suites: shared privacy for social networks. In Symposium on Usable Privacy and Security, 2009.

[11] A. K. Fabeah Adu-Oppong, Casey Gardiner and P. Tsang, "Social circles: Tackling privacy in social networks", In Symposium On Usable Privacy and Security, 2008.

[12] A. C. Squicciarini, S. Sundareswaran, D. Lin, and J. Wede, "A3p: Adaptive policy prediction for shared images over popular con-tent sharing sites," inProc. 22nd ACM Conf. Hypertext Hypermedia, 2011, pp.261–270.

[13] K. Strater and H. Lipford, "Strategies and struggles with privacy in an online social networking community," inProc. Brit. Comput. Soc. Conf. Human-Comput. Interact., 2008, pp.111–119.

[14] C. A. Yeung, L. Kagal, N. Gibbins, and N. Shadbolt, "Providing access control to online photo albums based on tags and linked data," inProc. Soc. Semantic Web: Where Web 2.0 Meets Web 3.0 at the AAAI Symp., 2009, pp. 9–14.

[15] S. Zerr, S. Siersdorfer, J. Hare, and E. Demidova, "Privacy-aware image classification and search," in Proc. 35th Int. ACM SIGIR Conf. Res. Develop. Inform. Retrieval, 2012, pp. 35–44.

[16] M. Wittie et al., "Exploiting Locality of Interest in Online Social Networks," Proc. CoNext, 2010.