Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 78 (2016) 114 – 119

Procedia Computer Science

International Conference on Information Security & Privacy (ICISP2015), 11-12 December 2015, Nagpur, INDIA

On Privacy and Security in Social Media – A Comprehensive Study

Senthil Kumar N*, Saravanakumar K, Deepa K

School of Information Technology and Engineering, VIT University, Vellore – 632014, India

Abstract

Social networks have become a part of human life. Starting from sharing information like text, photos, messages, many have started share latest news, and news related pictures in the Media domain, question papers, assignments, and workshops in Education domain, online survey, marketing, and targeting customers in Business domain, and jokes, music, and videos in Entertainment domain. Because of its usage by Internet surfers in all possible ways, even wee would mention the social networking media as the current Internet culture. While enjoying the information sharing on Social Medias, yet it requires a great deal for security and privacy. The users' information that are to be kept undisclosed, should be made private.

Peer-review under responsibility of organizing committee of the ICISP2015

Keywords: Social media; Privacy; Policy enforcement; Security;

1. Introduction

In the larger context of data mining, a considerable measure of productive analyzing so as to learn can be found advanced records of human conduct in interpersonal organizations without breaching the users' privacy. Thus, information ought to be made accessible in a manner that privacy should be safeguarded and protection is extremely scrutinized. On the other hand, the suspicion that any outsider which is intrigued to break down information can be viewed as reliable is truth be told unlikely, because of the key point of preference that the usage of all information, including recognizing and delicate ones, may provide for these gatherings. Due to the specific instance of interpersonal organizations, the most grounded measure that can be received is to make unflinching quality of individual's privacy who expresses the affiliation.

* Corresponding author. Tel.: +91-9943-541777.
E-mail address:senthilkumar.n@vit.ac.in

Peer-review under responsibility of organizing committee of the ICISP2015
doi:10.1016/j.procs.2016.02.019

According to the authors [3], who had proposed that any sort of examination about the number of inhabitants in clients who express inclinations, therefore defusing protection dangers as well as vital investigation. The proposition is still to keep connection ready to the interpersonal organization profiles of their users, however to permit clients to partner some guaranteed property estimations with their credentials, by picking each time they express credits that need to uncover. In the sideline perspective of the privacy domain [1], the subject of privacy has been under scrutiny and ensuring the basic importance given by the particular academic group has deemed to be vigilant. To ensure privacy of clients by recognizing characteristics, not by vulnerability based anonymization. Thus, despite the fact that from an only specialized viewpoint our answer is closer to privacy than protection in the long run, individual information of clients is ensured.

Further, unknown examination relating to different attributes of the general population who communicated such an inclination is saved with no danger for users' privacy, in light of the fact that there is no real way to relate such data to a specific user. Besides, the above prerequisites bring out what is given by particular revelation and bit responsibility approaches, yet an immediate utilization of such ways to deal with our case is not resolute since these mechanism would permit outsiders to follow the user, subsequently breaking namelessness. The issue is in this way not trifling. The key solution depends on a cryptographic convention whose privacy is primarily in view of the infeasibility of discrete logarithms and the power of somewhat blinded signatures [7]. As a matter of fact, we can consider Facebook that it is not just a positive relationship with an online substance additionally as center doled out by the social users. Maintaining privacy of the register users is the central role of the authorities and any deviation of policy given would totally wreck the organizational policy governance which in turn leads to serious havoc to the fundamental rights of society. In social media, some of the private data are shared by the user unknowingly or voluntarily. Sometimes, private details other than that are intentionally shared by the users are extracted from them extrinsically by offering them some benefits. Through the Location-Based Social Network Services (LBSNS) like FireEagle, Google Latitude, Nearby etc., you are able to identify the location of a person. Even you are able to identify the location of his/her friends [9].

2. Possible Threats and Privacy risk in Social Network Sites

As per the privacy analytics viewpoint, determinants would oversee the advantages and pertaining dangers that influence a user’s choice to unveil certain credentials. It additionally proposes that individuals are infrequently eager to forego some privacy for an adequate level of danger. By utilizing Social Networking Sites [4], people open themselves to different sorts of dangers that have the regular impact of breaking their privacy. It had witnessed that privacy may be attacked in a few ways if personal information is not utilized reasonably and dependably. The creators recommend that restricted in which protection can be attacked is through unapproved access to social user information because of privacy break or poor strategies disablement. In addition to that, they had estimated the privacy intrusion can likewise happen as optional utilization where information gathered for one design is utilized to meet different closures, without the learning or assent of the information proprietor. Nonetheless, if the proper information strategies and practices furnish people with control over the revelation and utilization of their own data, protection concerns can be intervened. In a comparable strand, the hypothesis stipulates that divulgence is certain to solid instruments that permit users to control the amount they uncover in light of their objectives, learning and mentalities toward protection. In the connection of online social range interpersonal communication, such limit regulation can be accomplished through the utilization of privacy settings [8]. These securities setting improve users' capacity to reveal the information and additionally paving way for giving information of settings to the need.

2.1. Breach of Information Disclosure

The major setback of the privacy concerns deals that the user credentials is similar to a social contract where the users trade their own data against financial or nonmonetary rewards. It is very obvious that judicious users will keep taking an interest in such a social contract the length of the advantages surpass the present and future dangers of exposure. The suggestion is reliable with the hypothesis, which sets that people settle on decisions that permit them to experience greatest advantages and minimize expenses. It has been set to utilize the desires to reveal the users information given on Social Networking Sites. Since the proposed goal goes for observing the impacts of intrinsic

advantages, divulgence aim is part into two construct: one measures user' pre-reward readiness to uncover while alternate measures their prize propelled ability to reveal. The nonappearance of intrinsic–extrinsic qualification [2] in earlier works implied that revelation goal could be measured specifically from important free develops.

3. Proposed Methodology for Privacy issues in Social Media Sites

The sole objective of the study is to connect the quantitative system with a specific end goal to spuriously investigate the social information of the potential users and acquire the much needed details such as demographic data, temporal data, user profile etc., of the respondents. To augment this process, we had taken a survey system that will be thoroughly utilized and disseminated to over more than 200 social media users and the populace will be dictated by the non–probability testing strategy. Spiral testing and respondent-driven examining have additionally permits analysts to make gauges about the interpersonal organization joining the shrouded populace to solicit them on the protection from the current social network communities. Hence, this comprehensive study has focused more on privacy concerns hinges on the social networks and jolt out the privacy breaches effectively. We had identified some of the privacy concerns that the social users can undertake before they uses the social sites and embed their privacy setting on the site to prevent any breach of violation.

3.1. Predicting the behavior of social media users

This study goes for discovering the privacy and privacy in social network sites locales recognition among Social Media clients [6]. A specimen of 250 understudies was chosen haphazardly from distinctive piece of the world. A net of 185 polls were filled effectively and returned. Almost 78% of the respondents were males, while about 22% of them were females .On the other hand, roughly 72 of respondents were in the age bunch 20-35 years of age. Be that as it may, the quantity of respondents in the age gatherings "between 28-41 practically got 19% where different gatherings 50 or more is right around zero. Instructive level played a high effect subsequent to 58% are four year certification and graduate degrees are 21%. The years of utilizing Internet think about the commonality of interpersonal organization on the grounds that from those are utilizing the web for over 10 years are 56% and in the event that we connect the use with nature of SN it indicates 51 % for decently recognizable and 49% for extremely well known . Then again 90% of this study populace is utilizing Facebook and 36 % utilizing IslamTag and 62% twitter so this is leeway for us to think about Facebook protection model.

3.2. Privacy Glitches and Concerns

As it was illustrated in Table 1 that when getting some information about privacy and how well they are mindful of protection and terms of conditions, 52% are modestly acquainted with the elements and redesigns in Social Media protection which was demonstrated that they are acquainted with the protection when 87% confine get to some for certain part in their profile. Be that as it may[2], in the matter of changing protection 43% change their privacy setting every so often which implies just if anything happened and 47% once in a while change their protection setting and the same goes for privacy and record setting.

In the Table 1 below, we had identified the different privacy mechanisms that the social media site offered to the users to set in and engage in the privacy concerned activities. There would be a wide range of discrimination persists in the social media sets in offering the privacy policies to the users and from the survey taken, it has largely been noted that many of the users of social media site has not concern more on their privacy settings and kept the privacy details as such created.

Table 1. Privacy concerns in Social Media site and its comparisons

Privacy options	FaceBook	Twitter	LinkedIn	Google+
Restrict the visibility of the active users	Yes	No	No	No
Set the control on how others can find you	Yes	Yes	Yes	No
Block the users for their photo tag	Yes	No	No	Yes

Set login Alerts	Yes	No	No	Yes
Block Spam Users	Yes	Yes	Yes	Yes
Control who can message you	Yes	No	Yes	Yes

3.3. Various Possible Threats in Social Networking Sites

The security issues and privacy concerns are the major requirements of the social networking sites. But there were many deadliest attacks persists in all these social networking sites and safeguarding the potential users from these heinous attack have been the challenging task of many social analyst and developers. The basic security attacks are classified into three categories.

- Privacy Breach - Find link between nodes and edges and possibly identify the relation between them.
- Passive Attacks - This is totally anonymous and undetectable.
- Active Attacks - Form the new nodes intrinsically and trying to connect to the linked nodes and gain the access to the other nodes.

Table 2 illustrates the clear depictions of various attacks in social media sites and given the possible solution to how to handle the attacks safely [10].

Table 2. Major attacks, sub-attacks, and possible preventive policies [10]

Major domain of attacks [10]	Sub-attacks	Solution to handle the attacks
Social Networking Infrastructure attacks	TCP SYN Flood Attack, Smurf IP Attack, UDP Flood Attack, Ping of death, Tear Drop	-Use Anti-Virus and Anti-Malware Software. -Install appropriate Intrusion Detection System.
Malware Attacks	Crimeware, Spyware, Adware, Browser Hijackers, Downloader, Tool Bars	-Use of Anti-Virus. -Do not go for unknown links, friends, applications, email attachments etc., -Disable Cookies, Sessions, ActiveX if unknown or no counter-measures available.
Phishing Attacks	Deceptive phishing (emails), Malware-based phishing, Keyloggers, Search engine phishing	-Examine the emails carefully. -Validate the source of the data. - Beware of ads with offers
Evil Twin Attacks	Social engineering attack	-Careful about having friends and sharing information. -Authenticate the user profile and share the data. -Try to completely understand the policies of having friends in the social networking sites.
Identity Theft Attacks	Dumpster diving	-Use complex passwords, avoid password re-usage. -Shred your email or documents properly.
Cyberbullying	Cyberbullying	-Do not acknowledge the messages that are intended to hurt or threat. -Save and Archive the messages as evidences. -Take all threats seriously -Do not share personal information with all users.
Physical Attacks	Impersonation, Harassment through messages	-Need a well defined social networking policy. -Background security and privacy checks. -Properly make use of privacy settings options.

3.4. Privacy Setup on Social Networking Sites

Social network sites destinations work to reinforce privacy settings. Facebook and other long range social communication destinations limit protection as a major aspect of their default settings. It's essential for clients to go into their client settings to alter their protection choices. These locales like Facebook give clients the alternative to not show individual data, for example, conception date, email, telephone number, and business status. For the individuals who decide to incorporate this material, Facebook permit clients to limit access to their profile to just permit the individuals who they acknowledge as "companions" to see their profile. Be that as it may, even this level of privacy can't keep one of those companions from sparing a photograph to their own PC and posting it somewhere else. Be that as it may, at present less social media site clients have constrained their profiles.

For example, let us take how the users to restrict the profile visibility to others in different social media sites:

- Facebook: Facebook's privacy setting for new users is set to Friends Only. To set this, visit Settings > Privacy > Who can see your future posts?
- Twitter**:** Settings > Security and privacy > Privacy > Tweet Privacy > Protect my Tweets.
- LinkedIn: To change this: Settings > Account > Helpful Links > Edit your public profile.
- Google+: To change this setting, type the name of a Circle in the "To" field below your post before you publish it.

Facebook could plainly express that they could give no assurances with respect to the privacy of their information, and that if clients make their profiles open, all data contained in that may be seen by occupation questioners and school chairmen.

Keep in mind most long range informal communication destinations encourage to quit applications, conceal companion rundown and shroud intrigues. However much of the data is still open as a matter of course. It is crucial that all long range interpersonal communication destinations clients limit access to their profiles, not post data of unlawful or arrangement disregarding activities to their profiles, and be wary of the data they make accessible.

4. Trust Management and Issues

Protection is a precondition for online self-divulgence, yet self-revelation additionally diminishes privacy by expanding the measure of online data accessible to different clients; the connections between these builds appear to be affected by critical variables, for example, trust and control [5]. Trust is characterized as the conviction that people, gatherings, or establishments can be trusted. It frequently has an opposing association with protection, if in light of the fact that individuals need to know data about others keeping in mind the end goal to trust them, which thusly has a beneficial outcome on online self-exposure.

Then again, the advancement of trust in an online domain is unpredictable on the grounds that the online world is characterized as frail. This is the reason a few studies have concentrated on the inclination of individuals to unveil data on the premise of both trust and protection. An imperative build that can impact this mind boggling relationship is the apparent control over data. For instance, word check, things constructed particularly, and prepared raters are regularly used to quantify online self-divulgence, and adjustments of instruments assembled for up close and personal correspondence are utilized to assess online trust.

4.1. Privacy Setup on Social Networking Sites

Late research has investigated the relationship between the online revelation of individual data and privacy concerns and the high hazard identified with online ruptures of protection. It was also well suggested that privacy is a term that is hard to characterize; legitimately, it alludes to one side to be not to mention, yet it can likewise incorporate the privilege to choose the degree to which individual data is revealed, the privilege to focus at the point when, how, and what data can be imparted to others . Finding that one's own particular private data has been scattered internet, including humiliating photographs or features that are recovered through phishing tricks or deficient protection limitations, speaks to a genuine mental danger. On Facebook, the setting is liquid and flimsy,

which has imperative ramifications in regards to the administration of privacy on Facebook. Clients' impression of their gathering of people are frequently thought little of as far as both size and scope, and the protection administration settings are regularly entangled, futile, and demand particular assessments. Privacy dangers are regularly thought little of, while the social advantages emerging from the revelation of individual data are frequently overestimated. Besides, online ruptures of privacy are as often as possible thought to be a working's piece of Facebook, and solicitations for individual data don't stress clients. These attributes of privacy administration impact web unveiling conduct and clients view they could call their own self-revelation.

5. Conclusion

It has been observed that privacy concerns are very feeble in the social networking sites and the users endeavours to make the appropriate changes on their social media privacy is substantially lower than other mode of security operations. Besides, many of the social media users have the dearth of technical makeovers and thus yield the low privacy concerns to their own content. In the statistics taken, we had identified many of the shortcomings and hiccups on the technical side of privacy and security measures are on the social media sites. Hence, we had given the possible root cause of the glitches and proposed the changes to take over for the privacy concerns of social networking site. If we would go for enforcing a set of well defined policies for social media, like, a strong password, awareness of changing password often, awareness of information disclosure, purpose of antivirus or related software, and proprietary software etc, we would secure the social networks from further attacks and vulnerabilities.

References

1. Basilisa Mvungi, Mizuho Iwaihara. Associations between privacy, risk awareness, and interactive motivations of social networking service users, and motivation prediction from observable features. *Computers in Human Behavior*, Dec 2014; 4(c):20-34.
2. Joshana Shibchurn, Xiangbin Yan.Information disclosure on social networking sites: An intrinsic – extrinsic motivation perspective. Computers in Human Behavior. 2015; 44:103-117.
3. Yan Li, Yingjiu Li, Qiang Yan, Robert H. Deng, Privacy leakage analysis in online social Networks, Computers and Security, Mar 2015; 49(c):239-254.
4. Patrick Van Eecke, Maarten Truyens, Privacy and social networks, *Computer Law & Security Review*;2010; 26(5):535-546.
5. Benson Vladlena, George Saridakis, Hemamali Tennakoon, Jean Noel Ezingeard, The role of security notices and online consumer behaviour: *An empirical study of social networking users*, *International Journal of Human Computer Studies*;Aug 2015; 80:36-44.
6. Yuan Li.Theories in online information privacy research: A critical review and an integrated framework, Decision Support System. June 2012; 54(1):471-481.
7. Nader Yahya Alkeinay, Norita Md. Norwawi. User Oriented Privacy Model for Social Networks. *International Conference on Innovation, Management and Technology Research, Malaysia*; 22 – 23 September, 2013; 191-197.
8. Gail-Joon Ahn, Mohamed Shehab, Anna Squicciarini. Security and Privacy in Social Networks. *IEEE Internet Computing*; 2011; 15(3): 10-12.
9. Paul Lowry, Jinwei Cao, Andrea Everard. Privacy Concerns versus Desire for Interpersonal Awareness in Driving the Use of Self-Disclosure Technologies: The Case of Instant Messaging in Two Cultures. *Journal of Management Information Systems;* 2011; 27(4):163-200.
10. Carl Timm, Richard Perez. Seven Deadliest Social Network Attacks. *Syngress Publishing*; 2010.