A Review of Security and Privacy Issues in Social Networking

A. A. Sattikar[#], Dr. R. V. Kulkarni[*]

[#] *V. P. Institute of Management Studies & Research, Sangli, Maharashtra, India*

[*] *Shahu Institute of Business Education & Research (SIBER), Kolhapur, Maharashtra, India*

***Abstract*— Online Social Networks have become an important part of daily digital interactions for more than half a billion users around the world. The various personal information sharing practices that online social network providers promote have led to their success as innovative social interaction platforms. At the same time, these practices have raised much critique and concerns with respect to privacy and security from different stakeholders. This work addresses the problem by presenting the analysis of different researches on security and privacy issues in social networking sites. After briefly summarizing these researches concerning security and privacy issues in SNSs, authors conclude with the role of Artificial Intelligence techniques such as Neural Network, Decision Tree techniques, Expert Systems and Adaptive Network based Fuzzy Inference System for privacy framework as a foundation to cope with security and privacy issues in their future research.**

***Keywords*— Social Network, Artificial intelligence, Neural Network, Expert System, Fuzzy Inference System**

I. INTRODUCTION

The Internet has become an evitable part of the lives of people today. Gone are the days when people would browse the net only to retain and even enhance their social lives through Social Networking Sites. These sites are an easy and cost effective way for people to reach out to their classmates, friends and family form across the globe. A large percentage of the success of these Social networking Sites can be attributed to the fact that they give individuals the opportunity to create their own space and a great way to connect with likeminded people, learn and share knowledge.

As mentioned, social networking often involves grouping specific individuals or organizations together. Social Networking covers a wide range of web based services that allows individuals to construct a public or semi-public profile within a bounded system. Further many Social Networking Sites (SNSs) commonly allow users to leave persistent comments on friend’s profiles and send private messages. In particular, SNSs are structured or personal networks, with individual at the center of their own community. Many of the SNSs are enhanced with multiple collaborative tools such as the personal profile and friendly links which are commonly supported by commercial web sites such as Friendster(2002), LinkedIn and MySpace(2003) and Facebook(2004) including the ability to post and share files, participate in discussion or blogs rather than SNSs like Flikr(2004) or YouTube(2005) with limited Social networking features of sharing content like digital pictures and video. Other Social Networking Sites have been developed which have higher usage including Orkut(2005), Bebo(2005) and QQ(2006). With the development of Twitter in 2006, Social Networking took a new twist that incorporated mobile phones into Social Networking.

Since the success of an SNS depends on the number of members, it attempts to encourage new users to register by improving the design of the website while security and privacy considerations are often left behind. As a consequence, third parties are using this information in different ways to undermine the privacy of SNS users. The privacy risks of this undesired access to profile information can vary from the creation of digital dossiers to stalking, identity theft, spam, cyber bullying, etc. As a response to different security and privacy related risks as well as to questions related to understanding of users' behavior and reasons for information disclosure, SNSs have been studied from different perspectives such as inference attacks, privacy inference, sociology, psychological studies, law, privacy policies, solutions to privacy protection, security issues and recommendations. Some researches offer an in-depth discussion on social network structure, privacy threats, trust and analysis of amount of disclosed information and user strategies for keeping their privacy intact.

By being aware of your cyber-surroundings and who you are talking to, you should be able to safely enjoy social networking online. Our research is directed at the issue of privacy risk and user behavior in order to suggest viable solutions for users to both improve their privacy protection, and be able to deploy the social functions expected from these types of network.

II. REVIEW OF LITERATURE

The researches on social networking sites so far are focused specifically on social network sites where some of these are connected to social media, social software, Web2.0, social bookmarking, educational technologies, communities research, etc. But with the development of social network sites, security protection of private information online has been a serious and important research topic. Hence the review concentrates following specific researches only on security and privacy of social network sites for investigation.

Gross, Ralph, and Acquisti, Alessandro. (2005)
They evaluate the amount of information they disclose and study their usage of the site’s privacy settings. They highlight potential attacks on various aspects of their privacy, and show that only a minimal percentage of users change the highly permeable privacy preferences.

Jones, Harvey, and Soltren, Jose Hiram. (2005).
Through their research they analyzed the Facebook system in terms of Fair Information Practices as recommended by the Federal Trade Commission. In light of the information

available and the system that protects it, they used a threat model to analyze specific privacy risks. Specifically intruders are exploiting security holes. For each threat, they analyzed the efficacy of the current protection, and where solutions are inadequate.

Gross and Acquisti (2005)
In one of the first academic studies of privacy and SNSs, they analyzed 4,000 Carnegie Mellon University Facebook profiles and outlined the potential threats to privacy contained in the personal information included on the site by students, such as the potential ability to reconstruct users' social security numbers using information often found in profiles, such as hometown and date of birth.

Acquisti, Alessandro, and Gross, Ralph. (2006).
Through their research on privacy concern, they found that some users manage their privacy concerns by trusting their ability to control the information they provide and the external access to it. However, researchers find significant misconceptions among some members about the online community's reach and the visibility of their profiles.

Barnes, Susan. (2006).
Their research results highlight the unexpected privacy consequences of the complex interactions among multiple data sources in modern information economies and quantify privacy risks associated with information revelation in public forums.

Stutzman's (2006)
A same theme is also explored in his research of Facebook users where description of the "privacy paradox" that occurs when teens are not aware of the public nature of the Internet. In analyzing trust on social network sites,

Hodge (2006)
He argued that the fourth amendment to the U.S. Constitution and legal decisions concerning privacy are not equipped to address social network sites. For example, do police officers have the right to access content posted to Facebook without a warrant? The legality of this hinges on users' expectation of privacy and whether or not Facebook profiles are considered public or private.

Dwyer, Catherine, Hiltz, Starr Roxanne, and Passerini, Katia. (2007).
The results of their research suggest that in online interaction, trust is not as necessary in the building of new relationships as it is in face to face encounters This study demonstrates online relationships can develop in sites where perceived trust and privacy safeguards are weak.

Lenhart, A., and Madden, M.. (2007).
In their research they commented that the majority of teens actively manage their online profiles to keep the information they believe is most sensitive 1away from the unwanted gaze of strangers, parents and other adults. While many teens post their first name and photos on their profiles, they rarely post information on public profiles they believe would help strangers actually locate them such as their full name, home phone number or cell number

Preibusch, Soren, Hoser, Bettina, Gürses, Seda, and Berendt, Bettina. (2007).
The objective of this research is to contribute to propose a framework for analyzing privacy requirements and for analyzing privacy-related data. They outline a combination of requirements analysis, conflict-resolution techniques, and a P3P extension that can contribute to privacy within such sites.

Jagatic, Johnson, Jakobsson, and Menczer (2007)
In another research examining security issues and SNSs, they used freely accessible profile data from SNSs to craft a "phishing" scheme that appeared to originate from a friend on the network; their targets were much more likely to give away information to this "friend" than to a perceived stranger.

Boyd (2007)
Privacy is also implicated in users' ability to control impressions and manage social contexts. Through his research, he asserted that Facebook's introduction of the "News Feed" feature disrupted students' sense of control, even though data exposed through the feed were previously accessible.

Chew, Monica, Balfanz, Dirk, and Laurie, Ben. (2008).
The researchers argued that the root of problems in the past has been a discrepancy between the mental model the user formed about the system, and how it actually worked. The key to solving the problems, then, is to align users' anticipations of the system with its actual workings.

Felt, Adrienne, and Evans, David. (2008).
This research by them addresses the privacy risks associated with social networking APIs by presenting a privacy-by-proxy design for a privacy preserving API that is motivated by an analysis of the data needs and uses of Facebook applications.

Guha Saikat, Tang Kevin, and Francis Paul. (2008)
This research presents a preliminary and partial answer to the general question "Can users retain their privacy while still benefiting from these web services?" Through a proof-of-concept implementation researchers demonstrate that NOYB(none of your business), a novel approach that provides privacy while preserving some of the functionality provided by online services, is practical and incrementally deployable, requires no changes to or cooperation from an existing online service, and indeed can be non-trivial for the online service to detect.

Krishnamurthy, Balachander, and Wills, Craig E.. (2008).
In this study they examined popular OSNs from a viewpoint of characterizing potential privacy leakage. Their study identifies what bits of information are currently being shared, how widely, and what users can do to prevent such sharing. Their long term goal was to identify the narrow set of private information that users really need to share on OSNs.

Lewis, K., Kaufman, J., and Christakis, N.. (2008).
Drawing upon a research based on Facebook, they argued that privacy behavior is an upshot of both social influences and personal incentives. Students are more likely to have a private profile if their friends and roommates have them; women are more likely to have private profiles than are men; having a private profile is associated with a higher level of online activity.

Debatin, Bernhard, Lovejoy, Jennette P., Horn, Ann-Kathrin, and Hughes, Brittany N. (2009).
This research investigates Facebook users' awareness of privacy issues and perceived benefits and risks of utilizing Facebook. Research found that Facebook is deeply integrated in users' daily lives through specific routines and rituals. Users claimed to understand privacy issues, yet reported uploading large amounts of personal information.

Ai Ho Maiga, A. Aimeur, E. (2009).
Their research examines the privacy protection issues on social networking sites (SNS) such as MySpace, Facebook and LinkedIn. Based on this study, they found that many users still are not aware of these threats and the privacy settings provided by SNS are not flexible enough to protect user data.

boyd, danah, , and Hargittai, Eszter. (2010).
This research examines the privacy concerns voiced following the sense of exposure and invasion. In essence, the ‘privacy trainwreck’ that people experienced was the cost of social convergence.

Brady Robards. (2010).
Their research on the Gold Coast, social network site in Australia argues that young users are consistent with developing increasingly complex strategies for managing their online privacy and social interactions.

Francesca Musiani. (2010).
This research addresses and analyses the "first steps" of applications at the crossroads between social networks and P2P networks. More specifically, it discusses how such applications anticipate modifications in the management of users’ right to privacy, by harnessing both anonymity and knowledge of identity – aspects generally identified with P2P networks and social networks, respectively – depending on the different functionalities and layers of the application.

Markus Huber, Martin Mulazzani, and Edgar R. Weippl. (2010).
Within this research, they present novel friend injection attack which exploits the fact that the great majority of social networking sites fail to protect the communication between its users and their services. The friend injection attack enables a stealth infiltration of social networks and thus outlines the devastating consequences of active eavesdropping attacks against social networking.

Raynes-Goldie, Kate. (2010).
This research explores how 20–something Facebook users understand and navigate privacy concerns. Based on a year–long ethnographic study in Toronto, Canada, this research looks at how — contrary to many mainstream accounts — younger users do indeed care about protecting and controlling their personal information.

Boyd, Danah, and Marwick, Alice. (2011).
Based on the Facebook, the research found that both frequency and type of Facebook use as well as Internet skill are correlated with making modifications to privacy settings. In contrast, it also observe few gender differences in how young adults approach their Facebook privacy settings, which is notable given that gender differences exist in so many other domains online.

Fuchs, Christian. (2011).
This research critisizes and introduces an alternative analytical framework for studying privacy on Facebook, social networking sites and web 2.0. This framework is connecting the phenomenon of online privacy to the political economy of capitalism—a focus that has thus far been rather neglected in research.

Raynes-Goldie. (2011).
Drawing on the existing body of primarily youth-focused research, particular focus is paid to the key debate around youth and privacy attitudes (the ‘privacy paradox’), with an examination of newer research on adults and social network use.

Hongyu Gao, Jun Hu, Tuo Huang, Jingnan Wang, Yan Chen (2011).
The researchers organized different security attacks into four categories - privacy breaches, viral marketing, network structural attacks, and malware attacks - and they offered an in-depth discussion of each category and analyze the connections among the different security issues involved.

The above mentioned researches on Social Network security and privacy issue deal with user’s concern for security and privacy issues whereas very few researches has made attempt for effectively detecting network security threats and optimally choosing methods and tools to get rid of their effects and damage with limited scope of network security threats.

But in today’s growing and ever changing world of social networks, network management systems need to have the abilities of intellectual reasoning, dynamic real time decision making, and experience based self-adaptation and improvement. Furthermore, ever increasing size and complexity of social networks require automation for their management systems. Automation minimizes human involvement which produces effective and time saving solutions for proper and dynamic supervision of these large and heterogeneous networks. In the light of above discussion, the design of an efficient, dynamic and automated social network management framework requires support from the field of artificial intelligence, which need further research. As the techniques based on the principles of artificial intelligence like Neural Network, Decision Tree techniques, Expert Systems and Adaptive Network based Fuzzy Inference, provide sophisticated abilities of intelligent decision making, experience based improvement and creative problem solving. The integration of AI techniques to solve current problems is a help to achieve intelligent environments offering adaptive behaviors depending on the user's intentions. With the above background in the mind, the researchers are intended to provide the role of modern techniques from the fields of Artificial Intelligence for improving Social Network management through their upcoming research.

REFERENCES

[1] Gross, Ralph, and Acquisti, Alessandro. (2005). Information Revelation and Privacy in Online Social Networks. Proceedings of WPES'05. (pp. 71-80). Alexandria, VA: Association of Computing Machinery (conference paper)

[2] Jones, Harvey, and Soltren, Jose Hiram. (2005). Facebook: Threats to Privacy. 6.805/STS085

[3] Gross, R., & Acquisti, A. (2005). Information revelation and privacy in online social networks. Proceedings of WPES'05 (pp. 71-80). Alexandria, VA: ACM.

[4] Acquisti, Alessandro, and Gross, Ralph. (2006). Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook.In Golle, P. and Danezis, G. (Eds.), Proceedings of 6th Workshop on Privacy Enhancing Technologies. (pp. 36--58).Cambridge, U.K. Robinson College. June 28-30.

[5] Barnes, Susan. (2006). A privacy paradox: Social networking in the United States. First Monday, 11 (9).

[6] Stutzman, F. (2006). An evaluation of identity-sharing behavior in social network communities. Journal of the International Digital Media and Arts Association, 3, 10-18.

[7] Hodge, M. J. (2006). The Fourth Amendment and privacy issues on the "new" Internet: Facebook.com and MySpace.com. Southern Illinois University Law Journal, 31, 95-122.

[8] Dwyer, Catherine, Hiltz, Starr Roxanne, and Passerini, Katia. (2007). Trust and Privacy Concern Within Social Networking Sites: A Comparison of Facebook and MySpace. Proceedings of AMCIS 2007. Keystone, CO. (conference paper)

[9] Lenhart, A., and Madden, M.. (2007). Teens, Privacy and Online Social Networks: How teens manage their online identities and personal information in the age of MySpace. (techreport)

[10] Preibusch, Soren, Hoser, Bettina, Gürses, Seda, and Berendt, Bettina. (2007). Ubiquitous social networks? Opportunities and challenges for privacy-aware user modeling. Proceedings of the Workshop on Data Mining for User Modelling at UM 2007. Corfu, Greece, June 2007. (conference paper)

[11] Jagatic, T., Johnson, N., Jakobsson, M., & Menczer, F. (2007). Social phishing. Communications of the ACM, 5(10), 94-100.

[12] boyd, d. (2007). Facebook's privacy trainwreck: Exposure, invasion, and social convergence. Convergence, 14 (1).

[13] Chew, Monica, Balfanz, Dirk, and Laurie, Ben. (2008). (Under)mining Privacy in Social Networks. (techreport)

[14] Felt, Adrienne, and Evans, David. (2008). Privacy Protection for Social Networking APIs. W2SP '08.

[15] Guha Saikat, Tang Kevin, and Francis Paul. (2008). NOYB: Privacy in Online Social Networks. Proceedings of the first workshop on Online social networks. (conference paper)

[16] Krishnamurthy, Balachander, and Wills, Craig E.. (2008). Characterizing Privacy in Online Social Networks. Proceedings of the first workshop on Online social networks. (conference paper)

[17] Lewis, K., Kaufman, J., and Christakis, N.. (2008). The Taste for Privacy: An Analysis of College Student Privacy Settings in an Online Social Network. Journal of Computer-Mediated Communication, 14(1), 79-100. (journal article)

[18] Debatin, Bernhard, Lovejoy, Jennette P., Horn, Ann-Kathrin, and Hughes, Brittany N.. (2009). Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences. Journal of Computer-Mediated Communication, 15 (1), 83 - 108. (journal article)

[19] Ai Ho Maiga, A. Aimeur, E. (2009). Computer Systems and Applications, IEEE/ACS International Conference, AICCSA 2009. 271 – 278. (conference paper)

[20] boyd, danah, , and Hargittai, Eszter. (2010). Facebook Privacy Settings: Who Cares?. First Monday, 15 (8). (journal article)

[21] Brady Robards. (2010). Randoms in my bedroom: Negotiating privacy and unsolicited contact on social network sites. PRism, 7(3). (journal article)

[22] Francesca Musiani. (2010). When Social Links are Network Links: The Dawn of Peer-to-Peer Social Networks and Its Implications for Privacy. Observatorio (OBS*), 4 (3), 185-207. (journal article)

[23] Markus Huber, Martin Mulazzani, and Edgar R. Weippl. (2010). Who On Earth Is Mr. Cypher? Automated Friend Injection Attacks on Social Networking Sites. Security and Privacy--Silver Linings in the Cloud, 1, 80--89. http://friendinjection.nysos.net (journal article)

[24] Raynes-Goldie, Kate. (2010). Aliases, creeping, and wall cleaning: Understanding privacy in the age of Facebook. First Monday, 15(1). (journal article)

[25] boyd, danah, and Marwick, Alice. (2011). Social Privacy in Networked Publics: Teens' Attitudes, Practices, and Strategies. Privacy Law Scholars Conference.Berkeley, CA May.

[26] Fuchs, Christian . (2011). An alternative view of privacy on Facebook. Information, 2 (1), 140-165. Special issue on "Trust and privacy in our networked world", edited by Dieter M. Arnold and Herman T. Tavani (journal article)

[27] Raynes-Goldie. (2011). Annotated bibliography: Digitally mediated surveillance, privacy and social network sites. (misc)

[28] Hongyu Gao, Jun Hu, Tuo Huang, Jingnan Wang, Yan Chen (2011). Internet Computing, IEEE 15(4), July-Aug. 201,1 56 – 63, (journal article)