Chapter 7

Information Security and Management in Social Network

Alkesh Patel
Rediff.com, India

Ajit Balakrishnan
Rediff.com, India

ABSTRACT

Social networking sites (SNSs) have gained significant attention in last few years. Most Internet users are associated with at least one popular SNS depending on their personal and professional preferences. Users have, in general, trusted the SNSs with personal data, and assumed that their privacy preferences are correctly enforced. Users of SNSs often want to manage the sharing of information and content with different groups of people based on their differing relationships. Configuring settings for each user is a great burden for a user, and most of the time, settings are not evident to users, and hence some automatic or semi-automatic mechanism should be available to reduce the privacy configuration efforts. Increasing user-driven contribution has also led to other kinds of problems, like spam and abusive message contents. The authors refer both of these types as social spam, which not only consumes extra resources of site, but also spoils the user experience and creates legal issues. In large scale SNS, human moderation becomes out of hand, and there is a need for machine intelligence to get rid of such spammers in an effective way. In social networks, users’ actions, contributions, demographic details, et cetera can be tracked, and necessary measures can be taken if unwanted behavior about a particular user is detected. One can make a user model of reputation to identify troublesome users and ban their activities temporarily or permanently whenever needed. User reputation systems help to improve the user experience of a site, enrich content quality, and provide incentives for users to become better, more active participants. In this chapter, authors describe issues related to privacy, social spamming, and show the measures to handle them by nearly automatic ways. The chapter also shows the making of a user reputation system and its applicability in social network.

DOI: 10.4018/978-1-4666-0197-0.ch007
INTRODUCTION

The success and growth of social networking sites like Facebook, Orkut and many other locally dominant sites are very apparent. Such sites provide users various tools to stay in touch with friends, family and colleagues where they can view and share updates, photos or any other interesting life transitions. At the time of registration to these sites, users are asked to provide basic information like name, school, college, company, email ids, phone, city, address etc. Moreover, users also perform lot of other activities e.g. commenting on feeds, photo/video/link sharing, updating profile information etc. There are settings provided to user for what kind of information will be visible to others and who can see that information. There is a tread off between encouraging interactions and enforcing strict privacy settings. Additionally, providing configuration for controlling each friend in the user’s network is complex and it rather confuses the users than helping them. In general, user would like to show certain information to everyone, only friends, friends of friends or none other than self. Automated approaches to grouping may have the potential to reduce this burden. However, their use remains largely untested. We shall discuss one of clustering methods in this chapter that group similar friends.

In social network, apart from users’ profile pages, there are fan pages where one can become a fan of a celebrity, location, organization or specific event so that he/she can get the updates from followed pages regularly. Many times page owners allow their page follower to post updates about them and discuss about it. Users behave nicely with their friends in online social network so there is hardly any need for moderation of comments but in case of fan pages, allowing users to become a fan, post whatever they like and discuss whatever they feel, can create unwanted situations. Some spammers try to seek attention of users on the most popular fan pages. It has also been seen that some users create fake profiles and try to put abusive remarks in discussion happening on active pages. Both of these cause very bad experience for genuine users and harm the reputation of not only page owner but also overall site. We call this phenomenon as social spamming and show automatic way of tackling them with the help of machine learning techniques in this chapter.

Web is moving from content-centric to user-centric gradually and social networking is the best example of it. In this chapter, we propose making of user reputation system which is capable of managing per user information management in effective manner and opens the doors to build potential related applications in social network.

In summary, the proposed chapter is supposed to provide thorough understanding with implementation details on following:

- Privacy issues and the automated ways to control them in social networks
- Social spamming issues and ways to tackle them
- Building user reputation system and its applications in social network

BACKGROUND

The networks of ‘Friends’ which users sustain on SNSs often consist of contacts associated with distinct facets of their lives. Presenting information equally across connections from these various implied groups can be problematic, particularly for users who are privacy conscious. Goffman (1959) observed that people attempt to maintain a great deal of control over their personas and minimize the appearance of characteristics that are contrary to an idealized version of them. Lampinen et al. (2009) study revealed that even the most carefree SNS users had attempted to manage group co-presence even when it was not explicitly supported by the system. This required establishing and continually managing group identities to facilitate more contextual sharing. Several stud-
Related Content

Teaching Systemic Risk: An In-Class Simulation for Diverse Audiences
[www.igi-global.com/article/teaching-systemic-risk/145365?camid=4v1a](www.igi-global.com/article/teaching-systemic-risk/145365?camid=4v1a)

The Compliance of IT Control and Governance: A Case of Macao Gaming Industry
[www.igi-global.com/article/the-compliance-of-it-control-and-governance/155103?camid=4v1a](www.igi-global.com/article/the-compliance-of-it-control-and-governance/155103?camid=4v1a)

Applying Game Theory in Securing Wireless Sensor Networks by Minimizing Battery Usage

Integrating Access Policies into the Development Process of Hypermedia Web Systems
[www.igi-global.com/chapter/integrating-access-policies-into-development/31087?camid=4v1a](www.igi-global.com/chapter/integrating-access-policies-into-development/31087?camid=4v1a)