Internationa Journa of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 3 | ISSN : 2456-3307

Malicious Detection in Social Media

Shivamurthy M. C, Sowmyashree K. M

MCA Department, P.E.S. College of Engineering, Mandya, Karnataka, India

ABSTRACT

We have entered the era of social media networks represented by Facebook, Twitter, YouTube and Flickr. Internet users now spend more time on social networks than search engines. Business entities or public figures set up social networking pages to enhance direct interactions with online users. Social media systems heavily depend on users for content contribution and sharing. Information is spread across social networks quickly and effectively. However, at the same time social media networks become susceptible to different types of unwanted and malicious spammer or hacker actions. There is a crucial need in the society and industry for security solution in social media. In this demo, we propose Social Spam Guard; a scalable and online social media spam detection system based on data mining for social network security. We employ our GAD clustering algorithm for large scale clustering and integrate it with the designed active learning algorithm to deal with the scalability and real-time detection challenges.

Keywords : Social Media, Malicious Detection, Facebook, Twitter, YouTube, Flickr, GAD, OSN, FW, ML

I. INTRODUCTION

The purpose of this document is to provide the software requirement specification report for the User we management thru filters in Open social Network. The intended audience stakeholders in the potential system' A System to exploit an M soft classifier to enforce customizable content-dependent Firs' Moreover, the flexibility of the system in terms of filtering options is enhanced through the management of BLs. Many studies have shown that average OSN user have difficulties in understanding the simple privacy settings provided by today OSNs. We decided to deal with this by exploiting data mining techniques to infer the best privacy preferences to suggest to OSN users, on the available social network data. In future, we intend to use similar techniques to infer BLs and Firs' Also we plan to study strategies and techniques limiting the inferences that a user can do on the enforced filtering rules with the aim of bypassing the filtering system.

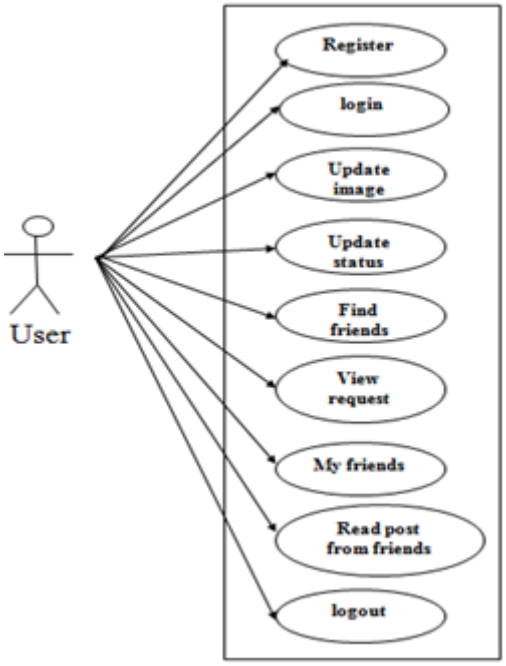

Figure 1. Use case of User

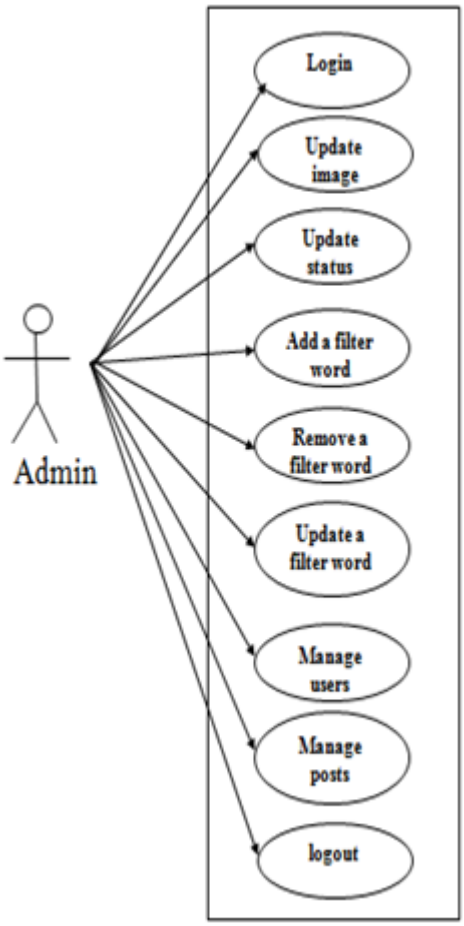

Figure 2. Sequence of Admin

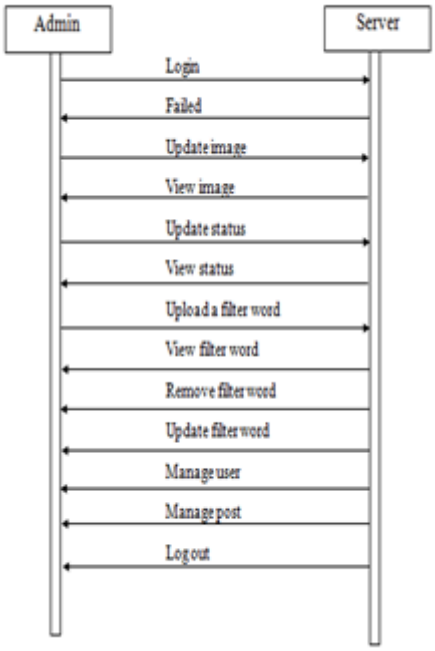

Figure 3. Use case of Admin

Figure 4. ER diagram

II. EXISTING SYSTEM

Indeed, today OSNs provide very little support to prevent unwanted messages on user walls. For example, Facebook allows users to state who is allowed to insert messages in their walls (i.e., friends, friends of friends, or defined groups of friends). However, no content-based preferences are supported and therefore it is not possible to prevent undesired messages, such as political or vulgar ones, no matter of the user who posts them.

III. PROPOSED SYSTEM

The aim of the present work is therefore to propose and experimentally evaluate an automated system, called Filtered Wall (FW), able to filter unwanted messages from OSN user walls. We exploit Machine Learning (ML) text categorization techniques to automatically assign with each short text message a set of categories based on its content.

FRs can support a variety of different filtering criteria that can be combined and customized according to the user needs. More precisely, FRs exploit user profiles, user relationships as well as the output of the M categorization process to state the filtering criteria to be enforced. In addition, the system provides the support

for user-defined Blacklists (BLs), that is, lists of users that are temporarily prevented to post any kind of messages on a user wall.

IV. CONCLUSION

In this paper, we have presented a system to filter undesired messages from OSN walls. The system exploits a ML soft classifier to enforce customizable content-dependent Firs' Moreover, the flexibility of the system in terms of filtering options is enhanced through the management of BLs.

V. REFERENCES

[1]. S. Ruj, M. Stojmenovic, and A. Nayak, "Privacy Preserving Access Control with Authentication for Securing Data in Clouds," Proc. IEEE/ACM Int'l Symp. Cluster, Cloud and Grid Computing, pp. 556- 563, 2012.

[2]. C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou, "Toward Secure and Dependable Storage Services in Cloud Computing," IEEE Trans. Services Computing, vol. 5, no. 2, pp. 220-232, Apr.- June 2012.

[3]. J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou, "Fuzzy Keyword Search Over Encrypted Data in Cloud Computing," Proc. IEEE INFOCOM, pp. 441-445, 2010.