

Secure Authentication Scheme for Social Networking

T. Primya¹, G. Kanagaraj², V. Suresh³, M. Krithika⁴

Assistant Professor, Dept of CSE, Dr. N.G.P. Institute of Technology, Coimbatore^{1,3}

Assistant Professor, Dept of CSE, Kumarguru College of Technology, Coimbatore²

Assistant Professor, Dept of IT, Dr. N.G.P. Institute of Technology, Coimbatore⁴

Abstract: A social networking service is an online platform that is used by people to build social networks or social relations with other people who share similar personal or career interests, activities, backgrounds or real-life connections. It plays a major role in our society. Privacy concerns with social networking services is a subset of data privacy, involving the right of mandating personal privacy concerning storing, re-purposing, provision to third parties, and displaying of information pertaining to oneself via the Internet. Maintaining privacy has a major problem, our proposed system provides additional security to the social network which is achieved by using Adaptive Privacy Policy Prediction (A3P). This system provides the privacy setting for the user. The features are selecting friend from friend list, follower request, news feed filtering, block the person and send the notification to the user when the violation is found. Our solution relies on an image classifier which may be related with similar policies, and on a policy prediction algorithm to automatically generate a policy for all the image, also according to users' social features.

Keywords: Networking Service, Policy Prediction, Filtering, Policy mining.

1. INTRODUCTION

The social network is a theoretical construct useful in the social sciences to study relationships between individuals, groups, organizations, or even entire societies (social units, see differentiation). The term is used to describe a social structure determined by such interactions. Social networking sites are varied and they incorporate a range of new information and communication tools such as availability on desktop and laptops, mobile devices such as tablet computers and smart phones, digital photo/ video/ sharing and "web logging" diary entries online. At present social networking are best place for sharing information between friends and relatives these sites help users to share daily in order, update daily news, share education information, update latest jobs postings etc. Users can get in touch with old friends and video chat with friends. Project design must be in Asp.net programming language and SQL server. Members should have secured user login and user's data must be private. Users must have features to search friends, send friend request, add friends, post comments and scraps, uploaded images, block, delete existing users. Quick progress in the world has given a different form for communication over the computers for the past few years. Apart from email, this form of interactions allows different users to share their information to the desired people all around the world through a common medium. The common example for such a medium is Social Networking, which is a web application used for incorporating different kinds of communities for people who share a common attention or actions.

The basic types of services that are provided by the social networks are communities, friends list, testimonial, and

the user's profile. Even chat sessions and number of applications are available today. Most likely Facebook has a notion of social proximity, which is one of their secret sauces. Think of every user on Facebook as a node and majority of these nodes are connected to other nodes via multiple relationship edges with friendship being the most common edge. Each of these edges must carry a certain weight and the sum total of them would be the social proximity score between two users. Privacy Policy Inference of User-Uploaded Images on Content Sharing Sites [1] Most content sharing websites allow user to enter their privacy preferences. Unfortunately, recent studies have shown that user struggle to set up and maintain such privacy policy setting. Design the interaction flows between the two building blocks to balance the benefits from meeting personal characteristics and obtaining community advice. Filtering is based on descriptions of administrator. [2] Filtering is considered as removing of data from an incoming content or finding data in that content. Content-based post filtering service for Online Social Networks (OSNs). Our system allows OSN users to have a direct control on the messages that are posted on their walls[2][3]. A user can follow any other user only with their consent[4]. If the user blocks a person, the shared content and the images of the user are not allowed to view by the blocked person[5]. If the defiance is occurred then the notification will send to the user[6]. In this generation, using online social network (OSN) is an unavoidable powerful weapon to exhibit peoples' views and ideas. We believe that the proposed strategy is a key service for social networks in that in today social networks users have little control on the posts displayed on their

walls. For example, Facebook allows users to filter the contents in their walls (i.e., friends, friends of friends, or defined groups of friends)[2]. Filtering is based on descriptions of administrator. Filtering is considered as removing of data from incoming content or finding data in that content.

A possible solution is to remove the unwanted messages from the user wall still retaining associates in the contact list. Considering the social media, the unwanted messages can be prevented, however retaining the associations in the contact list. User’s area of interest is largely blocked thus limiting the user choices and options [11]

In this paper an Adaptive Privacy Policy Prediction (A3P) system which endeavor to provide user highly secured privacy settings has been proposed. The role of image’s content and metadata. In general, similar images often incur similar privacy preferences, especially when people appear in the image. For example, one may upload several photos of his kids and specify that only the specified friends are allowed to see these photos.

2. EXISTING SYSTEM

The social network application existing does not provide service to filter messages according to user’s area of interest and also there is no data validation. Considering enormous number of messages in the user’s account, authenticating and authorizing each message and then removing them is a time-consuming task. The process becomes strenuous when huge number of messages reside in user’s inbox. Manual intervention is to be completely avoided.

3. RELATED WORK

Our work is related to privacy setting configuration in social networks and privacy analysis of online content sharing in social network.

2.1 Policy Prediction

The Policy Prediction algorithm is used to share the contents and images for friends, family members and co-workers through the social network. For example, Facebook. In our proposed system, we select friends from the friend list, that they only can view our shared contents and the uploaded images.

2.2 Filtered Wall

Content Based Filtering in online social network by exploiting ML techniques [2,3,6]The aim of the system is to experimentally appraise an automated system called Filtered Wall. It is able to filter unwanted messages from user wall which is achieved by using Flexible rule based system. The idea of proposed system is filtering the unwanted post from the home page in OSN wall.

2.3 Followers

A user can follow any other user, and the user being followed need not follow back. In facebook the user can

follow any others without their permission. Here we provide the follower request to follow others.

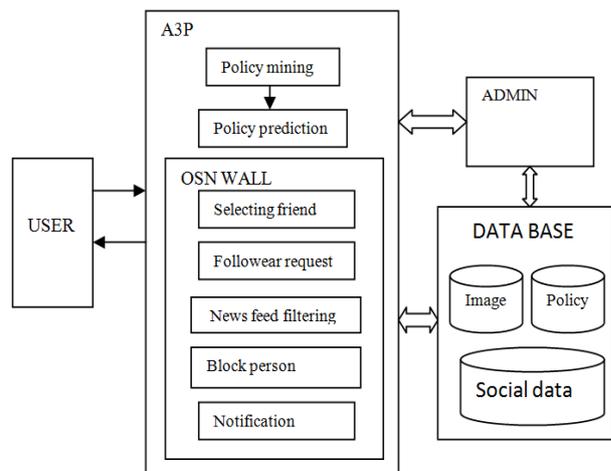
2.4 Notification

In Facebook, anyone can view our profile without our knowledge. In the proposed system if any violation is found, automatically it will send the notification to the concern account holder.

4. PROPOSED SYSTEM

In our proposed system, we provide additional security to the social network. For example, while uploading a photo privacy settings provided by Adaptive Privacy Policy Prediction System (A3P). In that all our friends, can view all the uploaded photo but we can have many friends in the friend list. In our proposal, we can select the number of friends who can view or access the detail can be selected from friend list. If unknown users view our profile means automatically the notification will send to the concerned account proprietor. In this paper, an A3P system which aims to provide users hassle free privacy settings experience by automatically generating personalized policies. The role of image’s content and metadata. In general, similar images often incur similar privacy preferences, especially when people appear in the image. For example, one may upload several photos of his/her kids and specify that only the specified friends are allowed to see these photos.

In our architecture user and admin plays a major role. Admin monitors N number of users and their policies, and also it monitors Online Social Network Wall and database of social network. Database is a collection of data. It is used to store large amount of data and retrieval of data which is shared in the social network. A3P has a collection of policy. These policies are created and controlled by the administrator.



Our policies are inspired by popular content sharing sites (Eg: Facebook), although the actual implementation depends on the specific content-management site structure and implementation. When a user uploads an image, the image will be first sent to the A3P. The A3P classifies the

policy mining and policy prediction, determines whether there is a need to invoke the A3P-social. In most cases, the A3P predicts policies for the users directly based on their historical behaviour.

3.1 Policy Mining

Hierarchical mining approach for policy mining is proposed. Our approach leverages association rule mining techniques to discover popular patterns in policies. Policy mining is carried out within the same category of the new image because images in the same category are more likely under the similar level of privacy protection. The basic idea of the hierarchical mining is to follow a natural order in which a user defines a policy. Given an image, a user usually first decides who can access the image, then thinks about what specific access rights should be given, and finally refine the access conditions such as setting the expiration date. Correspondingly, the hierarchical mining first look for popular subjects defined by the user, then look for popular actions in the policies containing the popular subjects, and finally for popular conditions in the policies containing both popular subjects and conditions.

3.2 Policy Prediction

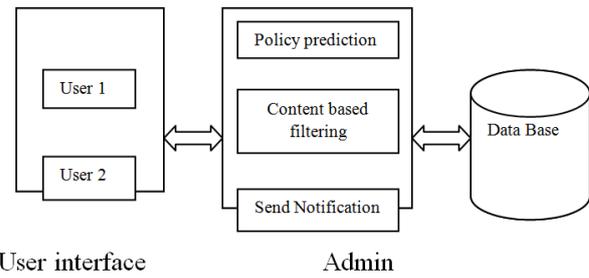
The policy mining phase may generate several candidate policies while the goal of our system is to return the most promising one to the user. Thus, an approach to choose the best candidate policy that follows the user's privacy tendency. It stores the user's policy performs the action according to it.

If the user accepts the policy which are presented in the Facebook settings, the administrator will send the YES decree to the database else if it is not found then the administrator will send the NO command to the database which are used for providing high security.

Selecting Friend: Used for selecting the friend from the friend list. Only these selected friends can view our shared contents and images. It will not be viewed by the unselected friends as it is filtered by the administrator.

Follower Request: User can send the follower request to anyone. Only if the request is accepted by that person, the user can follow him/her. Most content sharing websites allow users to enter their privacy preferences. Unfortunately, recent studies have shown that users struggle to set up and maintain such privacy settings. One of the main reasons provided is that given the amount of shared information this process can be tedious and error-prone. Therefore, many have acknowledged the need of policy recommendation systems which can assist users to easily and properly configure privacy settings.

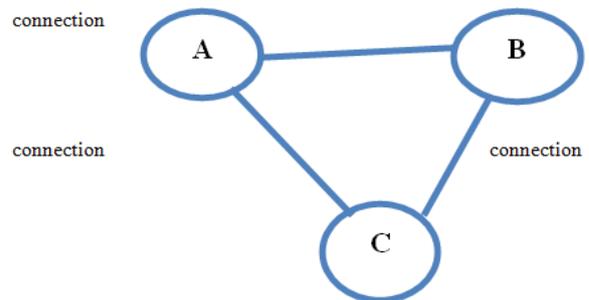
Newsfeed Filtering: In this system admin filters unwanted content in OSN wall, which is achieved by key word filtering technique. In this technique admin has a collection of keys, if that key matches with the user OSN wall that particular contents or post filtered by admin knowledge.



Block Person:

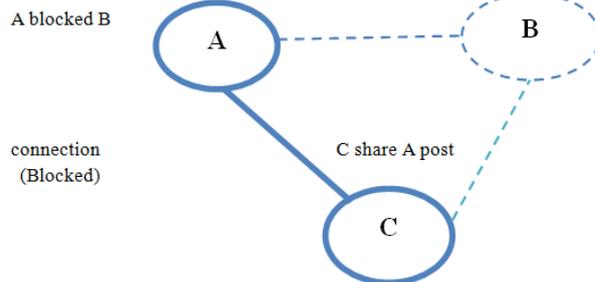
In before block: A,B&C are friends to each other. If anyone from the three friends share the images or the contents it can be viewed by the other two friends.

Before Block



In after block: If A blocks B, then the details of A will not be viewed by B, but A & C are friends, so the details of A can be viewed by C, but in our system through c also B cannot view the details of A.

After Block



Notification: Our proposed system has a notification feature, which is controlled by admin. If the violation occurs in any policy the notification send or indicate to the concern account holder.

Advantage:

The A3P-core focuses on analyzing each individual user's own images and metadata, while the A3P-Social offers a community perspective of privacy setting recommendations for a user's potential privacy improvement. The rule layer adopted for filtering unwanted posts has been introduced. When a user tries to access the image without permission, the owner receives an alerting message if it is blocked by OSN wall. If the violation is found, the notification will send to the user.

5. CONCLUSION

Proposed an Adaptive Privacy Policy Prediction (A3P) system that helps users automate the privacy policy settings for their uploaded images. The A3P system provides a comprehensive framework to infer privacy preferences based on the information available for a given user. It can effectively tackle the issue of cold-start, leveraging social context information. Our experimental study proves that our A3P is a practical tool that offers significant improvements over current approaches to privacy.

In this paper, Filtered Wall has been used. The flexibility of the system in terms of filtering options is enhanced through the management of Black Lists. System proposed in this paper represents just the core set of functionalities needed to provide a sophisticated tool for OSN message filtering with temporary blocking of user and also send notification, E-Mail to that who has posted unwanted message on wall. This might enhance services provided by OSN. Black List and Filtering Rule specification are made easier by development of GUI and a set of related tools. Along with it, our proposed system provides a better accuracy for classification of message as compare to previous implemented methods.

REFERENCES

- [1] Anna Cinzia Squicciarini, Member, IEEE, Dan Lin, Smitha Sundareswaran, and Joshua Wede, "Privacy Policy Inference of User-Uploaded Images on Content Sharing Sites" IEEE Transactions on knowledge and data engineering, vol. 27, NO. 1, January 2015 193
- [2] M. Vanetti, E. Binaghi, B. Carminati, M. Carullo and E. Ferrari "Content-based Filtering in On-line Social Networks" University of Insubria 21100 Varese, Italy.
- [3] Dhruv Vashistha, Sivagami G "Filtering Undesired Messages from Online Social Networks: A Content Based Filtering Approach" Dhruv Vashistha et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (2) 2014, 2046-2049.
- [4] Haewoon Kwak, Changhyun Lee, Hosung Park, and Sue Moon "What is Twitter, a Social Network or a News Media?" KAIST 335 Gwahangno, Yuseong-gu, Daejeon, Korea.
- [5] Prajakta Yerawar, Pankaj Agarkar "An advanced approach to avoid unwanted messages and blocking of person from OSN use" International Research Journal of Engineering and Technology (IRJET) Volume:
- [6] Preeti.C, Sara Anjum "Unwanted Message Filtration from OSN User's Wall and Blocking of Unwanted Person Using Trust Value" International Journal of Emerging Research in Management & Technology ISSN: 2278-9359 (Volume-5, Issue-1)02 Issue: 03 | June-2015.
- [7] M. Rabbath, P. Sandhaus, and S. Boll, "Analysing facebook features to support event detection for photo-based facebook applications," in Proc. 2nd ACM Int. Conf. Multimedia Retrieval, 2012, pp. 11:1–11:8.
- [8] 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.
- [9] S. Jones and E. O'Neill, "Contextual dynamics of group-based sharing decisions," in Proc. Conf. Human Factors Comput. Syst., 2011, pp. 1777–1786.
- [10] K.Babu and P.Charles, (2014) "A system to filter unwanted word using blacklists in social networks" International Journal of Computer Science and Information Technology, Vol. 5, (2), ISSN 09759646.

- [11] Macro Vnetti, Elisabetta, Binaghi, Elena Ferrari, Barbara Carminati and Moreno Carullo, (2013) "A system to filter unwanted messages from osn user wall" IEEE transaction on knowledge and data engineering, Vol 25.