Abstract

Social media’s become important part of our daily life. Using social media we are able to communicate with lot of people. Most popular example of social media which enable us to communicate with lot of people is Facebook. In which peoples have opportunities to meet new peoples, friends and communicate with each other. Peoples or users also share images, personal information through social site so maintaining privacy is a most important task. Because of large amount of image share through social sites image privacy is a major problem. There is a need of a tool which helps users to control access to their shared content. In this paper an Adaptive Privacy Policy Prediction is used to help user for privacy setting of their image. Our goal is to provide various privacy policy approaches to improve the Privacy of images or information shared in the social media sites.

1. INTRODUCTION

Nowadays sharing photos on Web is very popular. In many social sites such as Instagram user can upload their photos and also describe them by tags. While sharing their photos on these web sites users want their privacy. Currently, In most photo sharing sites users can only specify whether a photo is private, public or visible to their friends or those who are there family member. This setting can be applied by user to particular photo or a set of particular photos. They cannot share photos with only, for example, to those people who were participated in any particular event. If users move to another sharing site then list of...
friends also may have to compile again. In these website tags are widely used on photos. These tags are providing rich information about photos. So, by using tags assigned to the photos a better access control mechanism can be provided. Most content sharing websites allow users to enter their privacy preferences. But users have to struggle hard to set up such privacy. Maintenance of such privacy settings become very difficult [1]. This process can be error prone and tedious. In this paper, an Adaptive Privacy Policy Prediction (A3P) system is used to provide users privacy settings easily by automatically generating personalized policies. This system handles uploaded images by user.

Following criteria is used to influence privacy setting of image:

- **Personal characteristics and impact of social environment:** User’s social content can provide useful information about users. These content may be their profile picture and their relationship with other users. For example, users who are interested in photography may want to share photos with other photographer.

- **The role of image’s content and metadata:** In general, images which are of similar type require similar privacy preferences, mainly when people appear in the images. For example, one may upload photos of their Childs and want that only his family member can see and comment on these photo.

### 2. LITERATURE SURVEY

- **Jonathan Anderson** proposed Privacy Suites by which users can easily choose “suites” of privacy settings. This can be created by an expert using privacy programming. Through existing configuration of UIs it can be created directly. By exporting them to the abstract format also, privacy suites can be created. By existing distribution channels privacy suite is distributed to the members of the social sites. A rich programming language is less understand ability for end users. Motivated users should be able to verify a Privacy Suite by high level language. The main agenda is to maintain transparency.

- **Fabeah Adu-Oppong** uses the concept of social circles to develop privacy setting. This privacy setting provides a web based solution to protect personal information. The Social Circles Finder technique is used to automatically generate the friend’s list. This social circle of a person is analysed by this technique. It identifies intensity of relationship. This application identifies the social circles of the subject but not show them to the subject. The subject will then be asked questions about their willingness to share their personal information. Based on the answers the application finds the visual graph of users.

- **Kambiz Ghazinour** designed a system known as Your Privacy Protector [4]. It confirms the social net behaviour of their privacy settings. Recommending reasonable privacy options are also understands by this system. It uses user’s personal profile, User’s interests as parameters and by using this parameter the system constructs the personal profile of the user. It automatically learned profile of users and assign the privacy options. User see their current privacy settings on their social network with the help of this system, namely face book, and the possible privacy risks is monitor and detected. It adopts the necessary privacy settings based on the risks.
3. PROBLEM STATEMENT
There are numerous issues affected these e-services like security and privacy. They were many advanced projects carried for the privacy preserving policy for this social network. Since some unproductive algorithms produce advanced threatening may cause problem. Many observations were executed which failed to avoid the data exploitation and privacy problem. Most of the trouble we had studied in the existing system was acknowledged in terms of privacy and security of image data through the communication from one to an additional user in social network. one of the dangerous issues in these social networks is maintaining privacy. Since it is consistent and emerging service to communicate, it is also a new harass ground for data hackers, they can easily deteriorate the data.

4. EXISTING SYSTEM
There is an enormous body of work on image content analysis, for classification and interpretation retrieval and photo ranking also in the context of online photo sharing sites. Concluding of these works, existing work is probably the closest to ours. The Existing system distinguishes privacy-aware image classification using a mixed set of features, containing content and meta-data. This is however a binary classification which includes public as well as private involvement, so the classification task is very tedious to handle than ours. Existing proposals for automating privacy settings appear to be inadequate to address the unique image privacy needs due to the amount of information implicitly carried within contents, and their relationship with the online environment wherein Users struggle to set up and maintain privacy settings in the most content sharing websites.

5. PROPOSED SYSTEM

![Proposed System Architecture](image)

**Figure 1: Proposed System Architecture.**

5.1 Model
The perspective of Adaptive Privacy Policy Prediction (A3P) system to provide users a hassle free privacy settings experience by automatically generating personalized policies. Two main building blocks of the proposed A3P system is comprised as A3P-Social and A3P-Core. The focus of A3P-core is to analyzing each individual user’s own images and
metadata, the A3P-Social provide community perspective of privacy setting recommendations for a user’s potential privacy improvement. We design the interaction flows between two building blocks to balance the benefits from meeting personal characteristics and obtaining community advice.

5.2 Image Classification

Image Classifies hierarchical image classification which classifies images first based on their contents and after that refine each category into subcategories based on their metadata. If image have not metadata then it will be grouped only by content. Such as hierarchical classification gives a higher priority to image content and it minimizes the influence of missing tags. Multiple categories of some images are included as till they contain the typical content features or metadata of those categories that it is possible.

5.3 Mining

For policy mining we approach mining hierarchical mining. Our approach leverages in policies is association rule mining techniques to discover popular patterns. The same category of the new image the policy mining is carried out because similar level of privacy protection is provided in the same category of the image. The basic idea of the hierarchical mining is to follow a natural order in which a user defines a policy. When given an image, a user first decides who can access the image, then what specific access rights (e.g., view only or download) should be given is thinks by the user, and finally refine the access conditions. First search popular subjects defined by the user corresponding to the hierarchic mining, the search of popular actions in the policies containing the popular subjects, and finally both popular subjects and conditions which are containing by those polices that is the popular conditions.

6. COMPARISON OF EXISTING SYSTEM WITH PROPOSED SYSTEM

Figure 2: Comparison Of Existing System With Proposed System

We propose automation system in extracting and mining data, through the informal posts and chats on social media platforms, made by the user, in order to exactly know about
their concerns and issues, on a larger scale. As it has been seen, across several social media platforms, users are informally or casually posting about their concerns and feelings on the social media platforms and refrain from making such feelings or concerns available through feedbacks or surveys employed by the social media sites. In this system, the user images will be identified against certain standard data sets and several algorithms will be used in order to understand the relevance of their concern and feelings, through their posts or chats on the social media engine. The extraction of the social media content will be done by using standard APIs available on the internet. In this project we intend to develop data mining system for classification to demonstrate the work of social media data sense-making for privacy purpose, integrating both qualitative analysis and large-scale data mining techniques. This shows the diverse between existing and the proposed system. In the proposed system the access of the pages were limited when compared to existing system. Access control is by provided that access rights in a SN are limited to few basic constitutional rights, such as read, write and play for media content. This based type of approach which generates access-control policies from photo administration tags. Every photo is integrated with an access grid for mapping the photo with the participant’s friends. The contestant can select a suitable Partiality and access the information. Photo tags can be categorized as directorial or forthcoming based on the user needs.

7. CONCLUSION
This paper describes privacy policy techniques for user uploaded data images in various content sharing sites. Based on the user social behavior and the user uploaded image the privacy policy can apply. A3P system in used, which provide users easy and properly, configured privacy setting for their uploaded image. By using this we can easily prevent unwanted discloser and privacy violations. Unwanted discloser may lead to misuse of one’s personal information. Users automate the privacy policy settings for their uploaded images with the help of adaptive privacy policy prediction (A3P). Based on the information available for a given user the A3P system provides a comprehensive framework to infer privacy preferences. A3P system is a practical tool. An improvement over current approaches to privacy is offer by A3P.

8. ACKNOWLEDGEMENT
A dissertation of this magnitude has been a journey with various ups and downs. Whenever we are standing on most difficult step of the dream of our life, we often remember the great almighty god for his blessings kind help and he always helps us in tracking off the problems by some means on our lifetime. We feel great pleasure to represent this project mining social media data for understanding students learning experience. We would like to convey sincere gratitude to head of information technology engineering department Prof.P.V.Waje and our project guide Prof. S.A.Aher for her valuable guidance and support and who guided us and provided with her useful and valuable suggestions and without her kind co-operation it would have been extremely difficult for us to complete this desertion. We would like to convey sincere gratitude to B.E. coordinator Prof. R .S. Bhalerao for his valuable guidance and support. We would like to express our appreciation and thanks to Prof. Dr. G. B. Shinde, Principal, S.V.I.T, Nashik. Finally we are very
grateful to inspiring parents who loving and caring support contributes a major share in completion of our task.

9. REFERENCES