International Journal of Scientific Research and Management (IJSRM)
||Volume||5||Issue||06||Pages||5732-5738||2017||
Website: www.ijsrm.in ISSN (e): 2321-3418
Index Copernicus value (2015): 57.47 DOI: 10.18535/ijsrm/v5i6.50

Confidential Policy for Protecting User Images Uploaded on Shared Web Sites

***Akula Kiranmai*[1], *Gunisetti Loshma*[2]**
[1] M.Tech scholar, [2] Associate Professor.
[1,2] CSE, Sri Vasavi Engineering College, Tadepalligudem, India
[1] kiranmaiakula560@gmail.com, [2] loshma@gmail.com

Abstract

Along with the increase in the number of people using internet, the number of people sharing images across various web sites. One of the major issues with the sharing of images on public web sites is the unauthorized access of the content of the image. We propose a two-level framework which according to the user's available history on the site, determines the best available privacy policy for the user's images being uploaded.

We propose in this project non-recommended user can search and send the request of image to the administrator can accept the response and approve the access permissions.

A hierarchical image classification that classifies pictures initially based on their contents then refine every class into subcategories based mostly on their metadata. Such a hierarchical classification provides a higher priority to image content.

Key Words: confidentiaility, classifiaction, Data mining, two level framework.

I. Introduction

Data mining, the extraction of hidden predictive information from large databases, Data Mining is defined as the procedure of extracting information from huge sets of data. we can say that data mining is mining knowledge from data decisions. The automated, prospective analyses offered by data mining move beyond the analyses of past events provided by retrospective tools typical of decision support systems. Classification is a general process related to categorization , the process in which ideas and objects are recognized, differentiated, and understood. They scour databases for hidden patterns, finding predictive information that experts may miss because it lies outside their expectations.

Two – level framework according to user's previous history on the site for determining best available privacy policy for the images which are being uploaded. Our problem solution relies on an image classification framework for all the image categories which may be associated with the similar policies, and on a policy prediction to systematically generate a policy for each newly uploaded image, also according to the users' social features.[5] A hierarchical image classification that classifies pictures initially based on their contents then refine every class into subcategories based mostly on their metadata. A picture that does not have a metadata are going to be classified solely by content. Such a hierarchical classification provides a higher priority to image content and minimizes the influence of missing tags.

The content sharing sites have grown and participation of users also increased. As part of their participation lot amount of personal information are shared. Particularly young internet users share private images about themselves, their friends and classmates without being aware of the consequences. Photo sharing users often lack awareness of privacy issues. A variety of risks are faced by individuals, such as identify theft, stalking, embarrassment, and blackmail as a result of proliferation of personal data. [2]

Public Profiles: Profiles viewable to all people in a user's network. Users may still restrict access to individual pieces of information in the profile.

Private Profiles: Profiles that can only be viewed by a user's friends.

Search Profile: Profile information returned in search results. Users from separate networks may view full name, profile picture, friends list.

Consider a photo of a student's graduation ceremony, for example. It could be shared within a Google+ circle or Flickr group, but may unnecessarily expose the students, family members and other friends. Sharing images within online content sharing sites, therefore, may quickly lead to unwanted disclosure and privacy violations [3], [7]. The role of image's content and metadata. In general, similar images often incur similar privacy preferences, especially when people appear in the images. For example, one may upload several photos of his kids and specify that only his family members are allowed to see these photos. He may upload some other photos of landscapes which he took as a hobby and for these photos, he may set privacy preference allowing anyone to view and comment the photos.

Although online social networks are offering novel opportunities for interaction among their users, they seem to attract non-users' attention particularly because of the privacy concerns they raise. Such concerns may be well placed; however, online social networks are no longer niche phenomena[4].online social networks, security, access controls, and privacy are weak by design; the easier it is for people to join and to find points of contact with other users (by providing vast amounts of personal information, and by perusing equally vast amounts of data provided by others).

Privacy settings for newly uploaded images and search results. Such alert systems could be directly integrated into social photo sharing applications like Flickr or Facebook. A second aspect is privacy oriented search. , privacy-oriented search retrieves a set of relevant images, and re-orders them according to privacy In order to create a list of images ranked by privacy.

Need for the study

The article assumes a great need for the suggested practice at present because of the increase in number of privacy breaches reported during the study period. The author had approached the department of cyber security to understand the extent of damage caused by such privacy breaches.

Need For Social Networking:

Social networking is one of the major technological phenomenons of the Web, with hundreds of millions of attached users. Social network enables a form of self expression for the users and help them to socialize and share contents with others. Social networking sites are very useful in sharing information, making friends and keeping in touch with old friends. But with the increasing demand of social networking sites privacy concern is also increased.

With SNS, users engage with each other for various purposes, including business, entertainment and knowledge sharing. The commercial success of SNS depends on the number of users it attract, and by encouraging users to add more users to their network and to share data with others in SNS.

Need For Privacy:

Since SNS are widely in demand of current scenarios, the risk of their usage has also increased. Due to the lack of awareness among user and presence of less privacy protection tools, huge amount of user's data, including user's personal information, pictures and videos, is at risk. They can be used by strangers, content sharing is one of the main features of SNSs, but they do not provide any mechanism for collective enforcement of privacy policies on shared data. Privacy expectations in social networks are based on relationships. Typical social networks support friends and networks with privileged access. *Friends:* Friendships are a defining characteristic of social networking sites, and friends receive access to personal data. Friendships require acceptance by both parties. *Networks:* Social networks also support networks, where members have some access to each other. Bebo and Facebook associate access controls with school attendance. Alternately, self-defined regions can be considered a network, and privacy controls may be associated with the chosen location. *Public Visibility:* Sites define some subset of a profile (such as the user's name and affiliation) visible by default for searching and identification. Most sites also allow users to relax or strengthen their definition of public information. Past work demonstrates that users have strong expectations for privacy on social networking sites. In order to help users protect their personal data, the SNSs architecture adopts a simple user centric policy management approach, where a privacy aware user is able to specify a policy that manages access to their posted profile objects. There have been numerous studies concerning the privacy in the online world. A number of conclusions were drawn from these studies:

1. There are varying level of privacy control, depending on the online site. For e.g.: Some sites make available user profile data on the Internet with no ability to restrict access, while other sites

limit user profile viewing to a set of selected trusted friends [6].

2. The individuals lack appropriate information to make informed privacy decisions .

Due to lack of user awareness and proper privacy protection tools, huge quantities of user data, including personal information, pictures and videos are quickly falling into hands of authorities, strangers, recruiters and the public at large [6].

II. Related Work

Many social networking sites have begun building interfaces to support grouping, like Facebook lists and Google+'s "Circles." However, existing policy comprehension tools, such as Facebook Audience View, are not aligned with this mental model. PViz, an interface and system that corresponds more directly with how users model groups and privacy policies applied to their networks. PViz allows the user to understand the visibility of her profile according to automatically constructed, natural sub-groupings of friends, and at different levels of granularity [1].

As sharing personal media online becomes easier and widely spread, new privacy concerns emerge – especially when the persistent nature of the media and associated context reveals details about the physical and social context in which the media items were created. we use context-aware camera phone devices to examine privacy decisions in mobile and online photo sharing. Through data analysis on a corpus of privacy decisions and associated context data from a real-world system, we identify relationships between location of photo capture and photo privacy settings, several implications and opportunities for design of media sharing applications, including using past privacy patterns to prevent oversights and errors.[8]

At the time we deployed the survey, Facebook allowed users to manage the privacy settings of uploaded content (photos, videos, statuses, links and notes) using five different granularities: Only Me, Specific People, Friends Only, Friends of Friends, and Everyone. Specific People allows users to explicitly choose friends to share content with.The default or "recommended" privacy setting [7]. We deploy a survey, implemented as a Facebook application, to 200 Facebook users we find that 36% of content remains shared with the default privacy settings. We also find that, overall, privacy settings match users' expectations only 37% of the time, and when incorrect, almost always expose content to more users than expected. Finally, we explore how our results have potential to assist users in selecting appropriate privacy settings by examining the user-created friend lists.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 [2].

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. However, existing proposals for automating privacy settings appear to be inadequate to address the unique privacy needs of images [3], due to the amount of information implicitly carried within images, and their relationship with the online environment wherein they are exposed [6].

Popular photo-sharing sites have attracted millions of people and helped construct massive social networks. Contributing images to an interest group would greatly promote interactions between users and expand their social networks. In this work, we intend to produce automatic recommendations of a user's images to suitable photo-sharing groups Photo sharing websites such as Yahoo! Flickr® now allow and promote formation of interest groups. In such groups, the interactions naturally involve sharing pictures and videos of or related to the topics of interest. Within a large social network, contributing images to one or more interest groups is expected to greatly promote the personal social interactions of users and expand their personal social networks.[9]

Proposed Architecture

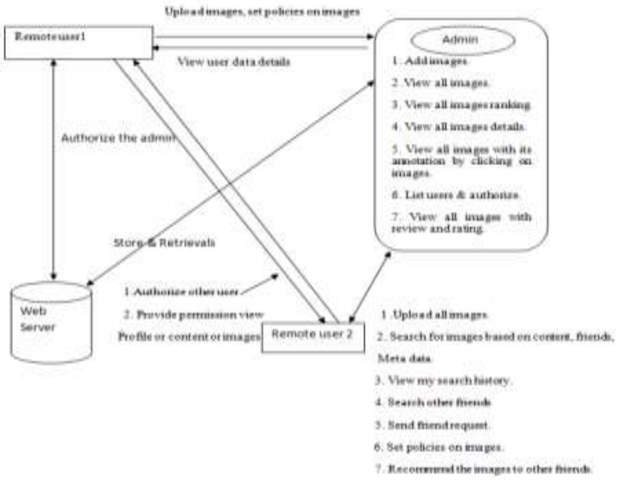

Upload images, set policies on images
Remoteuser1
View user data details
Admin
1. Add images
2. View all images.
3. View all images ranking
4. View all images details.
5. View all images with its annotation by clicking on images.
6. List users & authorize.
7. View all images with review and rating.
Authorize the admin
Store & Retrievals
Web Server
1. Authorize other user
2. Provide permission view
Profile or content or images
Remote user 2
1. Upload all images.
2. Search for images based on content, friends, Meta data.
3. View my search history.
4. Search other friends
5. Send friend request.
6. Set policies on images.
7. Recommend the images to other friends.

Figure 1: Proposed Architecture

III. Proposed Work

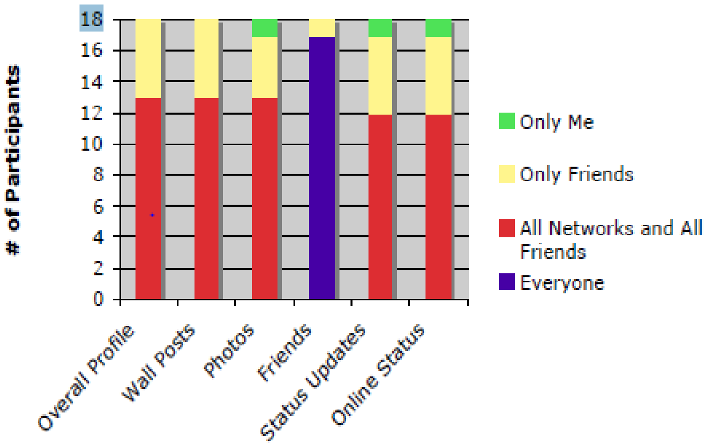
In this paper we suggest an alternative approach that Non recommended user accessibility for particular image. At present other recommended users only can view all the features of an image where as proposed system can be extended to view complete features of image.

The non recommended user first request to admin, the admin may provide accessibility based on max count of image views. and user can search or view image details , User can send friend request to other friends.

It helps people in giving access for sharing information to other people and also helps people in restricting the access on some other information which cannot be made public.

Our friends can share the data so we use an meta data.

IV. Results and Analysi



V. Conclusion and Future Enhancement

We proposed a two-level framework which

maintains user's available history on the site. In addition, in the system, non-recommended user can search and send the request of image to the administrator can accept the response and approve the access permissions. The results show the effectiveness of our concept classification and group/tag recommendation approaches. It provides a content sharing like text, image, audio, video, etc… With this emerging E-service for content sharing in social sites privacy is an important issue. It is an emerging service which provides a reliable communication, through this a new attack ground from an un-authored person can easily misuses the data through these media.

In Futher use the BIC algorithm to classify the attackers and the users with the help of the Access Policy Prediction and Access control mechanism. These provide a privacy policy prediction and access restrictions along with blocking scheme for social sites and improve the privacy level for the user in social media.

References

[1] A. Mazzia, K. LeFevre, and A. E.,, "The PViz comprehension tool for social network privacy settings," in Proc. Symp. Usable Privacy Security, 2012.

[2] K. Strater and H. Lipford, "Strategies and struggles with privacy in an online social networking community," in Proc. Brit. Comput. Soc. Conf. Human-Comput. Interact, 2008, pp.111–119.

[3] S.Ahern, D. Eckles, N. S. Good, S. King, M. Naaman, and R. Nair, "Over-exposed?: Privacy patterns and considerations in online and mobile photo sharing," in Proc. Conf. Human Factors Comput. Syst., 2007, pp. 357–366.

[4] A. Acquisti and R. Gross, "Imagined communities: Awareness, information sharing, and privacy on the facebook," in Proc. 6th Int. Conf. Privacy Enhancing Technol. Workshop, 2006, pp. 36–58.

[5] K. NITHYA , N. VENKATESWARULU," A Two- Level Framework for Protecting the Privacy of User Uploaded images on Content Sharing Sites"[online].Available: http://ijsetr.com/uploads/215634IJSETR12238-1463.pdf

[6] 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

[7]Y. Liu, K. P. Gummadi, B. Krishnamurthy, and A. Mislove, "Analyzing facebook privacy settings: User expectations vs. reality," in Proc. ACMSIGCOMM Conf. Internet Meas. Conf., 2011, pp. 61–70.

[8] S.Ahern, D. Eckles, N. S. Good, S. King, M. Naaman, and R. Nair, "Over-exposed?: Privacy patterns and considerations in online and mobile photo sharing," in Proc. Conf. Human Factors Comput. Syst., 2007, pp. 357–366.

[9] J. Yu, D. Joshi, and J. Luo, "Connecting people in photo-sharing sites by photo content and user annotations," in Proc. IEEE Int. Conf. Multimedia Expo, 2009, pp.1464–1467.

DOI: 10.18535/ijsrm/v5i6.50

About the Authors:

A.Kiranmai is pursuing M.Tech CSE in Sri Vasavi Engineering College in the branch of Computer Science and Engineering.

G.Loshma is currently working as an Associate Professor in CSE department of Sri Vasavi Engineering College.Her research area is text mining.