ISSN: 2321-7782 (Online)
Impact Factor: 6.047

Volume 4, Issue 7, July 2016

International Journal of Advance Research in Computer Science and Management Studies

Research Article / Survey Paper / Case Study

Available online at: www.ijarcsms.com

Privacy Policy Inference of User-Uploaded Images on Content Sharing Sites

K. Nithya[1]
Research Scholar,
H.H. The Rajah's College (Autonomous),
Pudukkottai, India

M. Muthuraman[2]
Research Guide,
H.H The Rajah's College (Autonomous),
Pudukkottai, India

Abstract: With the increasing volume of images users share through social sites, maintaining privacy has become a major problem, as demonstrated by a recent wave of publicized incidents where users inadvertently shared personal information. In light of these incidents, the need of tools to help users control access to their shared content is apparent. Toward addressing this need, we propose an Adaptive Privacy Policy Prediction (A3P) system to help users compose privacy settings for their images. We examine the role of social context, image content, and metadata as possible indicators of users' privacy preferences. 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. Our solution relies on an image classification framework for image categories which may be associated with similar policies, and on a policy prediction algorithm to automatically generate a policy for each newly uploaded image, also according to users' social features. Over time, the generated policies will follow the evolution of users' privacy attitude. We provide the results of our extensive evaluation over 5,000 policies, which demonstrate the effectiveness of our system, with prediction accuracies over 90 percent.

Keywords: Content Image; Photo Sharing; Privacy Policy Prediction; Social sites; Upload Image.

I. INTRODUCTION

The term "social media" refers to the wide range of Internet-based and mobile services that allow users to participate in online exchanges, contribute user-created content, or join online communities. Online social networks are websites that allow users to build connections and relationships to other Internet users. Social networks store information remotely, rather than on a user's personal computer. Social networking can be used to keep in touch with friends, make new contacts and find people with similar interests and ideas. The relation between privacy and a person's social network is multi-faceted. There is a need to develop more security mechanisms for different communication technologies, particularly online social networks. Privacy is essential to the design of security mechanisms. Most social networks providers have offered privacy settings to allow or deny others access to personal information details. In certain occasions we want information about ourselves to be known only by a small circle of close friends, and not by strangers. In other instances, we are willing to reveal personal information to anonymous strangers, but not to those who know us better. Social network theorists have discussed the relevance of relations of different depth and strength in a person's social network and the importance of so-called weak ties in the flow of information across different nodes in a network.

II. LITERATURE REVIEW

Sangeetha J et al Social media's become one of the most important part of our daily life as it enables us to communicate with a lot of people. Creation of social networking sites such as MySpace, LinkedIn, and Face book, individuals are given opportunities to meet new people and friends in their own and also in the other diverse communities across the world. Users of social-networking services share an abundance of personal information with a large number of "friends."

Nilesh Babu Maske et al we propose an Adaptive Privacy Policy Prediction (A3P) framework to assist clients with forming protection settings for their pictures. We inspect the part of social connection, picture substance, and metadata as could be allowed pointers of clients' security inclinations.

Aishwarya Sing et al 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 site.

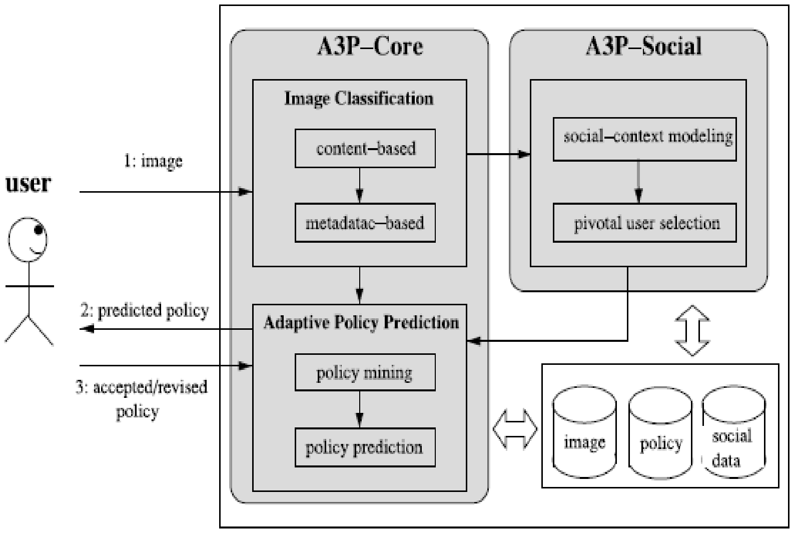
D. Priyadharshini et al This proposes a privacy policy prediction and access restrictions along with blocking scheme for social sites using data mining techniques. To perform this, the system utilizes APP (Access Policy Prediction) and Access control mechanism by applying BIC algorithm (Bayesian Information Criterion). Social network is an upgrading media for information sharing through internet. 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

III. Methodology

A. System Architecture:

The A3P system consists of two main components: A3P-core and A3P-social. The overall data flow is the following. When a user uploads an image, the image will be first sent to the A3P-core. The A3P-core classifies the image and determines whether there is a need to invoke the A3P-social. In most cases, the A3P-core predicts policies for the users directly based on their historical behavior. If one of the following two cases is verified true, A3P-core will invoke A3Psocial: (i) The user does not have enough data for the type of the uploaded image to conduct policy prediction; (ii) The A3P-core detects the recent major changes among the user's community about their privacy practices along with user's increase of social networking activities (addition of new friends, new posts on one's profile etc).

A3P Architecture



B. System Construction Module

The A3P system consists of two main components: A3P-core and A3P-social. The overall data flow is the following. When a user uploads an image, the image will be first sent to the A3P-core. The A3P-core classifies the image and determines whether there is a need to invoke the A3P-social. In most cases, the A3P-core predicts policies for the users directly based on their historical behavior. If one of the following two cases is verified true, A3P-core will invoke A3Psocial: (i) The user does not have enough data for the type of the uploaded image to conduct policy prediction; (ii) The A3P-core detects the recent major changes among the user's community about their privacy practices along with user's increase of social networking activities (addition of new friends, new posts on one's profile etc).

C. Content-Based Classification

To obtain groups of images that may be associated with similar privacy preferences, we propose a hierarchical image classification which classifies images first based on their contents and then refine each category into subcategories based on their metadata. Images that do not have metadata will be grouped only by content. Such a hierarchical classification gives a higher priority to image content and minimizes the influence of missing tags. Note that it is possible that some images are included in multiple categories as long as they contain the typical content features or metadata of those categories.

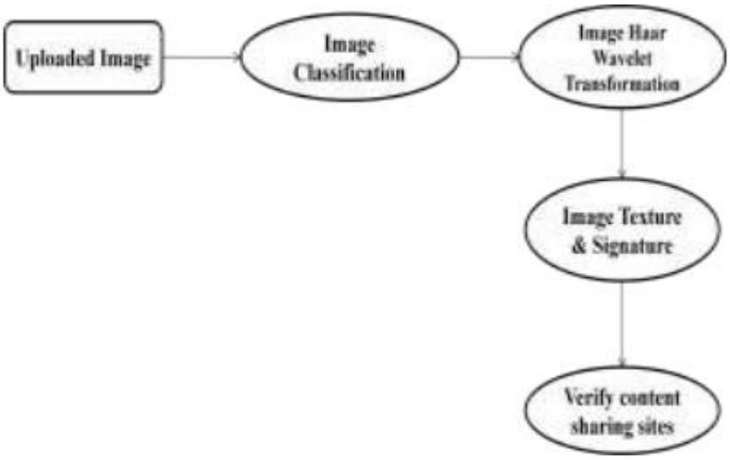

Uploaded Image
Image Classification
Image Haar Wavelet Transformation
Image Texture & Signature
Verify content sharing sites

Fig1. A3p- Content Based Classification

Our approach to content-based classification is based on an efficient and yet accurate image similarity approach. Specifically, our classification algorithm compares image signatures defined based on quantified and sanitized version of Haar wavelet transformation. For each image, the wavelet transform encodes frequency and spatial information related to image color, size, invariant transform, shape, texture, symmetry, etc. Then, a small number of coefficients are selected to form the signature of the image. The content similarity among images is then determined by the distance among their image signatures.

D. Metadata-Based Classification

The metadata-based classification groups images into subcategories under aforementioned baseline categories. The process consists of three main steps. The first step is to extract keywords from the metadata associated with an image. The metadata considered in our work are tags, captions, and comments. The second step is to derive a representative hypernym (denoted as h) from each metadata vector. The third step is to find a subcategory that an image belongs to. This is an incremental procedure. At the beginning, the first image forms a subcategory as itself and the representative hypernyms of the image becomes the subcategory's representative hypernyms.

E. Adaptive Policy Prediction

The policy prediction algorithm provides a predicted policy of a newly uploaded image to the user for his/her reference. More importantly, the predicted policy will reflect the possible changes of a user's privacy concerns. The prediction process consists of three main phases: (i) policy normalization; (ii) policy mining; and (iii) policy prediction.

IV. Algorithm Concepts

In authorization delegation models based on weighted directed graph, it is just as same as all authorization delegation models, resource access requests can be passed or not depends on "whether the certificate set *C* provided by the requester is able to demonstrate that the request set *r* is consistent with the local security policy *P*". It is the so-called compliance checking problem.

A. Definition of Data Structure Model

```
TYPE path=RECORD
trust: real;
pre: 0..n
END;
VAR
adj: ARRAY[1..n,1..n] OF real;
dist: ARRAY[1..n] OF path;
max:
 real;
k,i,u:1..n;
```

B. Algorithm Description

1) Input Items The serial number of the starting node V0 is given in the variable k, and the value of the trust field of the element in dist array indexed V0 is assigned with 100.

2) Output Items The maximum trust path from node V0 to every other node.

3) Steps of the Algorithm

```
1) [The initial nodes are divided into two groups]
(1) loop i step by 1,   from 1 to n
i) dist[i].trust←adj[k,i]
ii) if dist[i].trust≠0
then dist[i]. pre←k
else dist[i]. pre←0
(2) adj[k,k]←0
2) add the nodes in the second group to the first group one by one]
Loop until all nodes in the second group has been added into the first group
(1) [Find the node with the maximum trust value in the second group]
i) max←0;u←0
ii)loop i step by 1,   from 1 to n
if adj[i,i]=0 and dist[i].trust>max
then u←i;max←dist[i].trust
(2) [add the found node into the first group]
if u=0
```

```
then end algorithm [there is no node can be added to the first group]
else adj[u,u]←1
(3) [modify the trust value of node in the second group]
loop i step by 1,    from 1 to n
if adj[i,i]=0 and dist[i]. trust<dist[u]. trust×adj[u,i]/100
then begin
dist[i].trust←dist[u].trust×adj[u,i]/100;
dist[i].pre←u
end
```

V. Problem Statement

Consider social context such as one's friend list. While interesting, they may not be sufficient to address challenges brought by image files for which privacy may vary substantially not just because of social context but also due to the actual image content. As far as images, authors in have presented an expressive language for images uploaded in social sites. This work is complementary to ours as we do not deal with policy expressiveness, but rely on common forms policy specification for our predictive algorithm. In addition, there is a large body of work on image content analysis, for classification and interpretation, retrieval, and photo ranking, also in the context of online photo sharing sites. Of these works, probably the closest to ours. explores privacy-aware image classification using a mixed set of features, both content and meta-data. This is however a binary classification (private versus public), so the classification task is very different than ours. Also, the authors do not deal with the issue of cold-start problem.

VI. Implementation

A. Proof of the Algorithm

Division of the two groups and judging the trust value of nodes in the algorithm are clearly in accordance with the basic ideas above. The only thing to prove the correctness of this approach is to prove the division of the two groups and the trust value still meet the requirements after adding a node into the first group. That is to prove the trust value of the node V m is the maximum in the second group and the trust value is the greatest trust path value from the node V0 to Vm and Vm is the node of the greatest trust path value in the second group.

B. Policy Prediction

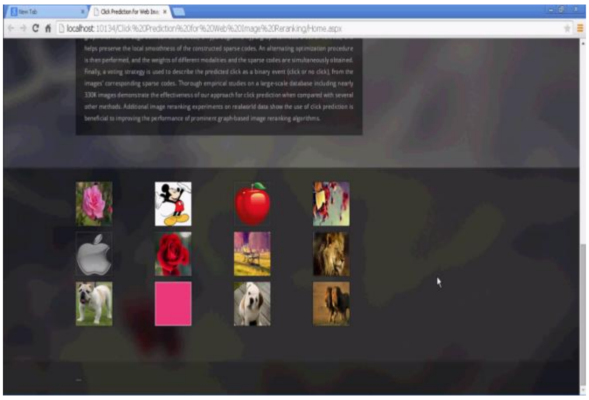
The policy mining phase may generate several candidate policies while the goal of our system is to return the most promising one to the user. Thus, we present an approach to choose the best candidate policy that follows the user's privacy tendency. To model the user's privacy tendency, we define a notion of strictness level. The strictness level is a quantitative metric that describes how "strict" a policy is. In particular, a strictness level L is an integer with minimum value in zero, wherein the lower the value, the higher the strictness level. It is generated by two metrics: major level (denoted as l) and coverage rate (a), where l is determined by the combination of subject and action in a policy, and a is determined by the system using the condition component. In all combinations of common subject and common actions are enumerated and assigned an integer value according to the strictness of the corresponding subjects and actions.

Therefore, we subtract (1-α) from l to obtain the final strictness level as shown in Equation:

$$L = l \ (1-\alpha)$$

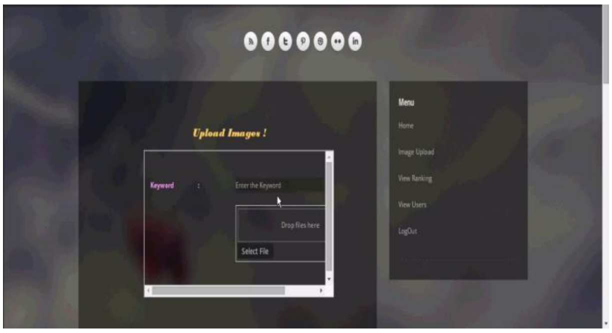
C. Results

Social media managers are often found in the marketing and public relations departments of large organizations. In face book, GUI is a type of user interface that allows users to interact with users through graphical icons and visual indicators such as secondary notation, as opposed to text-based interfaces, typed command labels or text navigation. GUIs were introduced in reaction to the perceived steep learning curve of command-line interfaces (CLI),which require commands to be typed on the keyboard.Well-designed graphical user interfaces can free the user from learning complex commandlanguages. On the other hand, many users find that they work more effectively with a commanddriven interface, especially if they already know the command language.

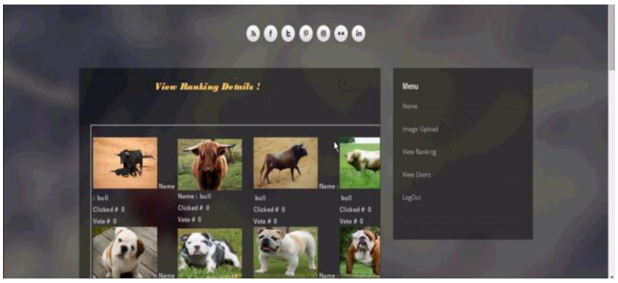

New Tab
Click Prediction for Web Ima
localhost:10134/Click%20Prediction%20for%20Web%20Image%20Reranking/Home.aspx

helps preserve the local smoothness of the constructed sparse codes. An alternating optimization procedure is then performed, and the weights of different modalities and the sparse codes are simultaneously obtained. Finally, a voting strategy is used to describe the predicted click as a binary event (click or no click), from the images' corresponding sparse codes. Thorough empirical studies on a large-scale database including nearly 330K images demonstrate the effectiveness of our approach for click prediction when compared with several other methods. Additional image reranking experiments on realworld data show the use of click prediction is beneficial to improving the performance of prominent graph-based image reranking algorithms.

Now apply the A3P core framework for sharing the image through the social book.it produce the privacy policy in this user can choose whom that want to share.



Here A3P social framework will apply in this,it deals with whether that particular image must be view or download to their shared people.



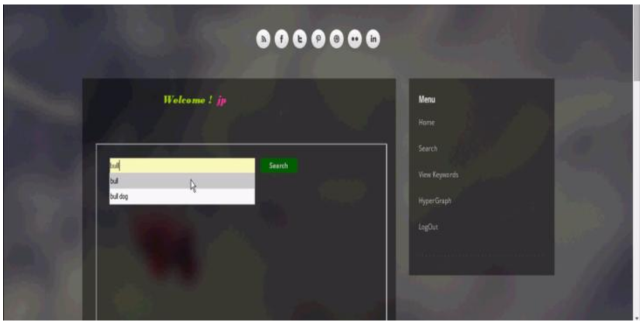
Name : bull
Clicked # 0
Vote # 0

Name : bull
Clicked # 0
Vote # 0

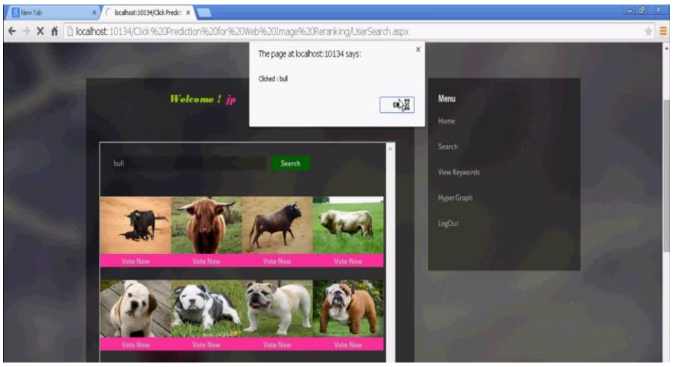
Name : bull
Clicked # 0
Vote # 0

Name : bull
Clicked # 0
Vote # 0

Image has been received by that particular user it show that image have the privacy of social book , that means if it have that privacy policy is applied .in that two options are available one is downloaded and another one is view. Downloaded option means people can have the permission to download image. At the same time view option have the permission to view alone.



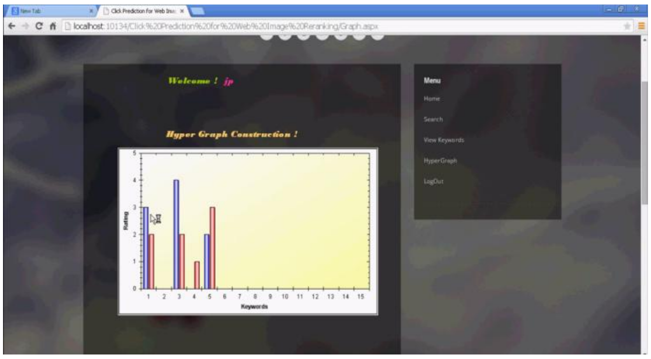
Commend has been blocked in the since for posting comment for the image, posted by the user that comment was unwanted that is negative word posted to that image means that commends will blocked(hidden to their friends)It done by the short text classification.


New Tab
localhost:10134/Click Predic
localhost:10134/Click%20Prediction%20for%20Web%20Image%20Reranking/UserSearch.aspx
Welcome ! jp
bull
Search
Vote Now
Menu
Home
Search
View Keywords
HyperGraph
LogOut

The page at localhost:10134 says:

Clicked : bull

In this method, we design an automated system, called Filtered Wall (FW), able to filter unwanted messages from OSN user walls. The architecture in support of OSN services is a three-tier structure. The first layer commonly aims to provide the basic OSN functionalities (i.e., profile and relationship management). Additionally, some OSNs provide an additional layer allowing the support of external Social Network Applications (SNA)1. Finally, the supported SNA may require an additional layer for their needed graphical user interfaces (GUIs)


New Tab
Click Prediction for Web Ima
localhost:10134/Click%20Prediction%20for%20Web%20Image%20Reranking/Graph.aspx
Welcome ! jp
Hyper Graph Construction !
Rating
0
1
2
3
4
5
Keywords
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
Menu
Home
Search
View Keywords
HyperGraph
LogOut

VII. Conclusion and Future Work

A. Conclusion:

In this proposed a system of adaptive prediction privacy policy (A3P), helps users automate their privacy uploaded image configuration. The information base for Privacy Preferences A3P system provides a comprehensive framework to infer a particular user on. We also effectively solve the problem of cold start, use of information in the social environment. Our experimental results show that our A3P is a handy tool, over current methods to provide significant improvements in privacy.

B. Future Work:

To further refine the context model and validate its generality and expressiveness by applying it to a set of versatile use cases. At the same time, this system working on the integration of trust aspects in the context model. For the privacy decision engine, this system currently working on suitable context and knowledge representations to enable efficient reasoning and inference of preferences and policies on different abstraction levels. We plan to implement the privacy decision engine in a prototype system to evaluate the accuracy of privacy decisions in user studies.

References

1. A Survey on the Privacy Settings of User Data and Images on Content Sharing Sites by Sangeetha J
2. Secure Photo Sharing on OSN by Nilesh Babu Maske , Sainath Tukaram Zariwad , Vijay Udhavrao Jogdand , Prof. Kiran Somase
3. A Survey on User-Uploaded Images Privacy Policy Prediction Using Classification and Policy Mining by Aishwarya Sing , Bhavesh Mandalkar , Sushmita Singh , Prof. Yogesh Pawar.
4. Yourprivacyprotector: A Recommender System For Privacy Settings In Social Networks by Kambiz Ghazinour , Stan Matwin, and Marina Sokolova.
5. An improved Privacy of User Data and Images on Content Sharing Sites using BIC by D. Priyadharshini , Smrina Das
6. D. G. Altman and J. M. Bland ,“Multiple significance tests: The bonferroni method,” Brit. Med. J., vol. 310, no. 6973, 1995.
7. J. Bonneau, J. Anderson, and L. Church, “Privacy suites: Shared privacy for social networks,” in Proc. Symp. Usable Privacy Security, 2009.
8. J. Bonneau, J. Anderson, and G. Danezis, “Prying data out of a social network,” in Proc. Int. Conf. Adv. Soc. Netw. Anal. Mining., 2009, pp.249–254.
9. H.-M. Chen, M.-H. Chang, P.-C. Chang, M.-C. Tien, W. H. Hsu, and J.-L. Wu, “Sheepdog: Group and tag recommendation for flickr photos by automatic search-based learning,” in Proc. 16th ACM Int. Conf. Multimedia, 2008, pp. 737–740.
10. M. D. Choudhury, H. Sundaram, Y.-R. Lin, A. John, and D. D. Seligmann, “Connecting content to community in social media via image content, user tags and user communication,” in Proc. IEEE Int. Conf. Multimedia Expo, 2009, pp.1238–1241.