ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 20, April 2016

Privacy Policy Inference in Social Sites Sharing Images with Access Control using Akaike Information Criterion

P.Kottai Selvam[1]
M.Phil Research Scholar,
Department of Computer Science and Engineering,
Alagappa University,Karaikudi, Tamilnadu
kottaibed1991@gmail.com

Dr.E.Ramaraj[2]
Professor,
Department of Computer Science and Engineering,
Alagappa University,Karaikudi, Tamilnadu
eramaraj@rediffmail.com

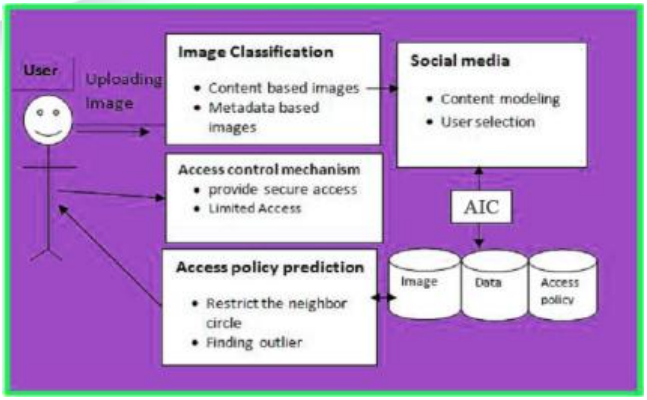
***Abstract*— In social sites faced more privacy problems that becomes a major issue, because increasing volume of images from users. It is emerging service which provides a reliable communication. Communication is a new attack ground for data hackers and they can easily misuses the data through these media. The role of social context, image content, and metadata are analyzed in this paper for indicators of users privacy preferences. The solution relies on an image classification framework for image which may be associated with similar policies, and on a policy prediction algorithm which automatically generate a policy for each newly uploaded image, also according to users' social features. This proposes a privacy policy prediction and access restrictions along with blocking scheme for social sites using data mining techniques. To perform this, AIC (Akaike Information Criterion) algorithm is applied to the system which utilizes APP(Access Policy Prediction) and Access Control Mechanism.**

Keywords*— *Privacy Policy Prediction, web-based services Introduction

I.INTRODUCTION

Now images are one of the key enablers of user's connectivity. Social sharing sites (e. g., Google+, Flickr, Facebook or Picasa) become one of the most remarkable parts of the daily life as it allows us to communicate with a group of people. Its helps outside of self expression for users, and helps them to entertain and exchange content with other users through social media's providing E-Service. The aggregated user information can result in unexpected exposure of one's social sharing sites and lead to mistreatment of one's personal information. 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. End users are nevertheless often not aware of the size or nature of the spectators accessing their data and the sense of understanding created by organism among digital friends often leads to disclosures that may not be suitable in a public forum. Such an open accessibility of data exposes in SN, The users obtain a number of security and privacy risks. In this area, propose and A3P (Adaptive Privacy Policy Prediction) system which target to provide user, users a disturb free privacy settings experience by generating personalized policies automatically and provide access control for users. Goal is to improve the set of privacy policy controls and defaults, but Research are restricted by the reality that there has been no in-depth study of users' privacy settings [1], [2], [3], [4]on sites like Facebook. While significant privacy disobedience and mismatched user expectations are likely to exist, the extent to which such privacy disobedience arises has yet to be quantified.

Corresponding to the aforesaid two criteria, the proposed A3P system is comprised of two main building blocks (as shown in Fig. 1): The A3P-core focuses on gathering each separate user's own images and metadata, while the A3P-Social offers a community view of privacy setting recommendations for a user's possible privacy improvement.



ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 20, April 2016

Fig.1 System Architecture

Users regularly sharing the data and images in Social Sharing Sites by this happening the privacy of the images may lock with the un-wanted parties. Hackers can chop the images through these social media so the privacy of the user images may loss. Today, for every single quantity of content sharing sites like Facebook—every wall post, photo, status update, and video—the up loader must settle on which of his friends, group members, and other Content Sharing Sites users should be intelligent to access the content. As a result, the problem of isolation on sites like Content Sharing Sites has received significant concentration in both the research society[4] and the mainstream media. Goal is to improve the set of privacy controls and defaults, but Research are restricted by the reality that there has been no in-depth study of users' privacy settings on sites like Content Sharing Sites. While significant privacy disobedience and mismatched user expectations are likely to exist, the extent to which such privacy disobedience arises has yet to be quantified [5].

II. RELATED WORK

Research Work is related to works on privacy setting design in social sites, recommendation systems, and privacy analysis of online images and Access control from other users.

A. Privacy Setting Configuration

The concept of privacy suites which propose to users a suite of privacy settings that "expert" users or other believed friends have already set, so that normal users can either directly choose a setting or only need to do small adjustment. A Machine-learning based approach to robotically extract privacy settings from the social context within which the data is formed. The wizard asks users to first assign privacy labels to selected friends, and then uses this as input to build a classifier which classifies friends based on their profiles and robotically assign privacy labels to the unnamed friends. Their results are in line with research approach: tags created for directorial purposes can be repurposed to help create logically correct access-control rules.

B. Recommendation Systems

The concept of privacy suites which propose to users a suite of privacy settings that "expert" users or other believed friends have already set, so that normal users can either directly choose a setting or only need to do small adjustment. A Machine-learning based approach to robotically extract privacy settings from the social context within which the data is formed. The wizard asks users to first assign privacy labels to selected friends, and then uses this as input to build a classifier which classifies friends based on their profiles and robotically assign privacy labels to the unnamed friends. Their results are in line with research approach: tags created for directorial purposes can be repurposed to help create logically correct access-control rules.

For example, proposes an interesting experimental evaluation of several collaborative filtering algorithms to recommend groups for Flickr users. These approaches have a totally different goal to our approach as they focus on sharing rather than protecting the content.

III.A3P FRAMEWORK

A. Preliminary Notions

Users can communicate their privacy preferences about their content exposé preferences with their socially connected users via privacy policies. The define privacy policies according to Definition 1.Research policies are motivated by popular content sharing sites (i.e., Facebook, Picasa, Flickr), although the actual implementation depends on the specific content-management site structure and implementation.

Definition 1. *A privacy policy P of user u consists of the following elements:*

- *Subject (S): A set of users socially connected to u.*
- *Data (D): A set of data items shared by u.*
- *Action (A): A set of actions granted by u to S on D.*
- *Condition (C): A boolean expression which must be satisfied in order to perform the granted actions.*

In the definition, users in S (Subject) can be represented by their identities, roles (e.g., family, friend, coworkers), or association (e.g., non-profit association, profit association). D (Data) will be the set of images in the user's profile. Each image has a particular ID along with some associated metadata like tags "tourism", "birthday". Images can be more grouped into albums. As for A, Researcher considers common types of actions: {view, comment, tag, download}. Last, the condition component C specifies when the granted action is valuable. C is a Boolean expression on the grantees' attributes like time, location, and age.

B. System Overview

The A3P system consists of two main blocks: A3P-social and A3P-core. On the entire data flow is the following. When user wants to upload an image in this system A3P core got that image and do some process. This A3P core classifies the data

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 20, April 2016

of image and determines here is a required to invoke the A3P Social. In such cases, the A3P- core predicts polices for the user straight based on their past actions. If one of the following two cases is verified true, A3P-social will invoked by A3P-core: (i) The user do not have enough data for uploaded image types to conduct policy prediction; (ii) The A3P-core detects the recent main changes in the middle of the user's group of people about their privacy practices along with user's enlarge of social networking activities (addition of new friends, new posts on one's profile etc).

C. A3P-Core

A3P-core have two major elements: (i) Adaptive policy prediction and (ii) Image classification. For every user, images are first classified based on content and metadata. Then, privacy policies of each category of images are analyzed for the policy prediction.

D. A3P-Social

The A3P-social employs a multi-criteria inference mechanism that produce representative policies by leveraging key information related to the user's social context and his general attitude toward privacy. As mentioned earlier, A3P-social will be invoked by the A3P-core in two scenarios. One is when the user is a newbie of a site, and does not have enough images stored for the A3P-core to infer meaningful and customized policies. The other is when the system notices important changes of privacy trend in the user's social circle.

V.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.

MODIFIED A3P FRAMEWORK

The concept of Access control mechanism is implemented additionally in the proposed modified A3P framework.

A. Image Classification

To obtain groups of images that may be associated with similar privacy preferences, in 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. Moreover, Fig. 2 shows an example of image classification for 10 images named as A, B, C, D, E, F, G, H, I, J, respectively. The content-based classification creates two categories: "nature" and "school". Images C, D, E and F are included in both categories as they show student like nature which satisfy the two themes: "nature" and "school". These two categories are further separated into subcategories based on tags associated with the images. As a result, they obtain two subcategories under each theme respectively. The image G is not shown in any subcategory as it does not have any tag, image A shows in both subcategories.

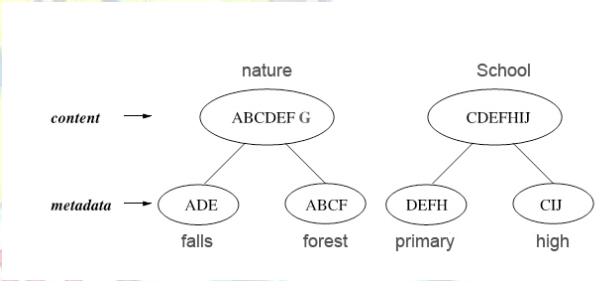


Fig.2 Two-level Image Classification

B. Content-Based Classification

The approach to content-based classification is based on an efficient and yet exact image similarity approach. Specifically, the 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.

C. Metadata-Based Classification

The metadata-based classification groups images into subcategories under aforementioned baseline categories. The process consists of three main steps.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 20, April 2016

1. The first step is to extract keywords from the metadata associated with an image. The metadata considered in the work are tags, captions, and comments.

2. The second step is to obtain a representative hypernym from each metadata vector.

3. The third step is to find a subcategory that an image belongs to. This is an incremental procedure.

D. Access Policy Prediction

Accessing the personal data in E-service make available an information distribution diagonally the world and at the same time it not working the privacy of the user data. Access policy is for retrieving the data or image in the network. By this kind of right of entry privacy may loss. For this problem the user of the social media compute the normalized and prejudiced average of the ratings of the users in the district. User have to confine the neighbor circle so un-wanted may not influence the data . User have to envisage the neighbor circle and provide a limited admission technique they have to choose 1) what information one disclose about oneself, and (2)who can access that information.When it comes to the usage of the data, the owner should be knowledgeable about the principle and purpose for which the data is organism or will be used and to provide a partiality. They have to set the level of regular to predict using (Fig.1).

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.we introduce the computation of the coverage rate a which is designed to provide fine-grained strictness level. a is a value ranging from 0 to 1 and it will just adjust but not dominate the previously obtained major level. In particular,

TABLE 1
Major Level Look-Up Table

Major Level	Subject	Action
0	family	view
1	family	comment
2	family	tag
3	family	download
4	friend	view
5	friend	comment
6	friend	tag
7	friend	download
8	coworker	view
9	coworker	comment
10	coworker	tag
11	coworker	download
12	stranger	view
13	stranger	comment
14	stranger	tag
15	stranger	download

we define a as the percentage of people in the specified subject category who satisfy the condition in the policy. For example, a user has five family members documented in the system and two of them are kids. When he specifies a policy with the condition age > 18, only three family members will satisfy this condition. The corresponding a is then 3=5 ¼ 0:6. The larger the value of a, the more people are allowed to access the image and the policy is less restricted. Therefore, we subtract (1-a) from 1 to obtain the final strictness level as shown in Equation (1):

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

The change on the policy preferences being more than four is considered prominent as it exceeds one quarter of the maximum strictness level.As time evolves, the average strictness levels in each category form a curve as shown in Fig. 3, where values of strictness levels are interpolated in-between any consecutive policy updates. Similarly, the outlier policies may form their own curves as denoted in the figure.

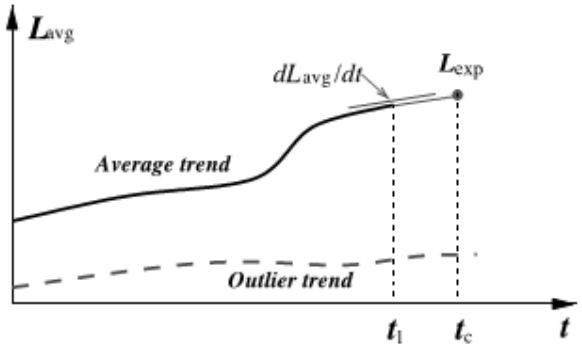


Fig. 3. Average strictness level curve.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 20, April 2016

E. Access control mechanism

Access control in the shared environment is one of the essential one. To supply a secure access Research have to limit the unauthorized user in these networks. Access control mechanism (ACM) is one of the privacy conserve one. ACM permit users to oversee access to information controlled in own spaces, users, unhappily, have no control over data be inherent in outside their spaces. For example, Facebook allows label users to eliminate the tags associated to their profiles or

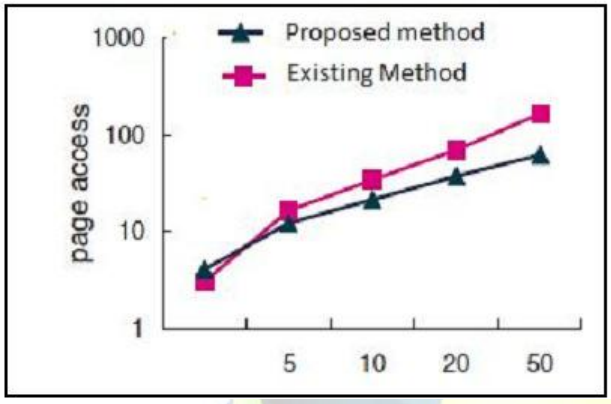


Fig.4 Difference between Existing and Proposed

report contravention asking Facebook managers to eliminate the contents that they do not want to split among the public. 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 Social Networks 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.

F. Akaike information criterion (AIC)

The Akaike information criterion (AIC) is good for prediction for data models. It is Relative quality of Statistical models in measure for set of data in Akaike information criterion. It is an asymptotically proficient model selection criterion. As $n \rightarrow \infty$, with probability approaching one, the model with the less AIC score will also possess the least Kullback-Leibler divergence. It is an asymptotic rough calculation; one should consider whether it applies before using it. That is Linear regression models and function approximation. The used following types of models in AIC, that are Generalized linear models Autoregressive Moving Average models, spectral estimation for data.

G. The generalized linear model

The Generalized Linear Model (GLM) is a flexible generalization of ordinary linear regression that allows for response variables that have error distribution models other than a normal distribution. The GLM generalizes linear regression by allowing the linear model to be related to the response variable via a link function and by allowing the magnitude of the variance of each measurement to be a function of its predicted value.

H. Autoregressive Moving Average models

Autoregressive–moving-average (ARMA) models provide a parsimonious description of a (weakly) stationary stochastic process in terms of two polynomials, one for the auto-regression and the second for the moving average.

The general form for calculating AIC:

Let L (Likehood) be the maximum value of the likelihood function for the model; let k be the number of estimated parameters in the model.

AIC = -2*ln(Likelihood) + 2*K

VI.CONCLUSION

Content Sharing Sites 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. 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. We also effectively tackled 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. For this issue Research recommendation systems use the AIC 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.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 20, April 2016

References

[1] J. Bonneau, J. Anderson, and L. Church, "Privacy suites: Shared privacy for social networks," in Proc. Symp. Usable Privacy Security, 2009.

[2] H. Lipford, A. Besmer, and J. Watson, "Understanding privacy settings in facebook with an audience view," in Proc. Conf. Usability, Psychol., Security, 2008.

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

[4] L. Church, J. Anderson, J. Bonneau, and F. Stajano, "Privacy stories Confidence on privacy behaviors through end user programming," in Proc.5th Symp. Usable Privacy Security, 2009.

[5] Sangeetha. J ,Kavitha. R, "An Improved Privacy Policy Inference over the Socially Shared Images with AutomatedAnnotation Process"

.