REVIEW PAPER ON PRESERVING PRIVACY POLICY OF USER UPLOADED IMAGES ON DATA SHARING SITES

Shital J. Mehatre [1], Prof. N. R. Chopde [2]

[1]SGBAU, Amravati University, G.H. Raisoni College of Engg & Management,
Anjangaon Bari Road, Amravati, 444701, India
[2]Professor N. R. Chopde, Dept. of Computer Science & Engineering,
G.H. Raisoni College of Engg & Management,
Anjangaon Bari Road, Amravati, 444701, India

---***---

Abstract - *As a recent time, the study shows that incidents where users inadvertently shared personal information through social media goes on increasing but with no or low privacy context. As there is increasing use of images for sharing through social sites, web document, web sites maintaining privacy has become a major problem. In light of these incidents, the need of tools to aid users control access to their shared content is necessary. This problem can be proposed by using an Privacy Policy Prediction system to help users compose privacy settings for their shared images. For examining the indicators of users privacy preferences one can use the role of social context, image content, and metadata as possible according to information available. Our solution relies on an image classification framework for image categories which may be associated with similar policies, and on a policy prediction algorithm for generate a policy for each newly uploaded image, this can be done according to user's social features. This will generate policies that will follow the evolution of user's privacy according to his requirement.*

***Key Words*: Privacy-preserving policy, classification framework, image content, Feature Extraction.**

1.INTRODUCTION *(Size 11 , cambria font)*

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. IMAGES are now one of the key enablers of users' connectivity. Sharing takes place among previously established groups of known people or social circles[1] (e. g., Google+, Flickr or Picasa), and also increasingly with people outside the users social circles. Semantically rich images may reveal content sensitive information. Sharing images within online content sharing sites, therefore, may quickly lead to unwanted disclosure and privacy violations. The aggregated information can result in unexpected exposure of one's social environment and lead to abuse 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.

Therefore, many have acknowledged the need of policy recommendation systems which can assist users to easily and properly configure privacy settings [5]. However, existing proposals for automating privacy settings appear to be inadequate to address the unique privacy needs of images, due to the amount of information implicitly carried within images, and their relationship with the online environment wherein they are exposed. Recommender systems can be defined as programs which attempt to recommend the most suitable privacy policy to particular users by predicting a user's interest in an content based on related information about the image. The aim of developing recommender systems is to reduce information overload by retrieving the most relevant information and services from a huge amount of data, thereby providing personalized services. The most important feature of a recommender system is its ability to "guess" a user's preferences and interests by analyzing the behavior of this user and/or the behavior of other users to generate personalized recommendations. A main feature is the process of segmentation which is used for the extraction of the main features of the image, like a color input, calculates the number of remaining points of the maps for color, brightness, contrast and orientation at different scales of static image. Segmentation means dividing a digital image into segments. Segmentation is to simplify the display of an image into something that's meaningful and easier to analyze change.

2. LITERATURE SURVEY

Jonathan Anderson proposed a paradigm called **Privacy Suites [2]** which allows users to easily choose "suites" of privacy settings. A privacy suite can be created by an expert using privacy programming. Privacy Suites could also be created directly through existing configuration UIs or exporting them to the abstract format. The privacy suite is distributed through existing distribution channels to the members of the social sites. The disadvantage of a rich programming language is less understandability for endusers. Given a sufficiently high-level language and goodcoding practice, motivated users should be able to verify a Privacy Suite. The main goal is transparency, which is essential for convincing influential users that it is safe to use. Fabeah Adu-Oppong developed privacy settings based on the concept of **social circles [3]**. It provides a web based solution to protect personal information. The technique named Social Circles Finder, automatically generates the friend's list. It is a technique that analyses the social circle of a person and identifies the intensity of relationship and therefore social circles provide a meaningful categorization of friends for setting privacy policies. The application will identify 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 a piece of their personal information. Kambiz Ghazinour designed a recommender system known as **YourPrivacyProtector [4]** that understands the social net behavior of their privacy settings and recommending reasonable privacy options. It uses user's personal profile, User's interests and User's privacy settings on photo albums as parameters and with the help of these parameters the system constructs the personal profile of the user. It automatically learned for a given profile of users and assign the privacy options. It allows users to see their current privacy settings on their social network profile, namely Facebook, and monitors and detects the possible privacy risks. Alessandra Mazzia introduced **PViz Comprehension Tool[5]**, better than other current policy comprehension tools Facebook's Audience View and Custom Settings page. A system that creates access-control policies from photo management tags, Peter F. Klemperer developed **a tag based access control of data[6]** shared in the social media sites. Ching-man Au Yeung proposes **decentralised authentication protocol[7],** a access control system, descriptive tags and linked data of social networks in the Semantic Web. Sergej Zerr propose a **Privacy-Aware Image Classification and Search[8]** to automatically detect private images, and to enable privacy-oriented image search. It combines textual meta data images with variety of visual features to provide security policies. In this the selected image features (edges, faces, color histograms) which can help differentiate between natural and man-made objects/scenes (the EDCV feature) that can indicate the presence or absence of particular objects (SIFT). It uses various classification models trained on a large scale dataset with privacy assignments obtained through a social annotation game. Anna Squicciarini developed an **Adaptive Privacy Policy Prediction (A3P)** system, a free privacy settings system by automatically generating personalized policies. The A3P handles user uploaded images based on the person's personal characteristics and images content and metadata. The A3P system consists of two components: A3P Core and A3P Social. 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. The disadvantage is inaccurate privacy policy generation in case of the absence of meta data information about the images. Also manual creation of meta data log data information leads to inaccurate classification and also violation privacy.

3. PROPOSED WORK

Our methodology of Policy Recommendation System consists of the following main building blocks – Saliency map, Classifier, Policy Match.

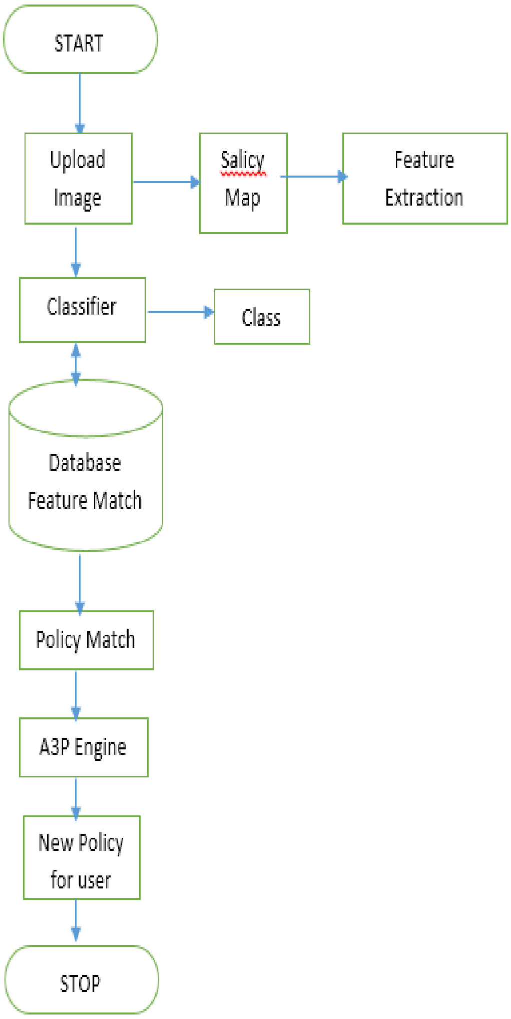

Fig -1: System Overview

The given flow graph shows how the proposed model will work-

Upload Image : User will upload the images having Objects and background.

Saliency map : Extract the object that is foreground image and suppressed the background to improve the classification accuracy using foreground features. For this we will use Saliency map which will help to extract features from images.

Feature Extraction : Extracting foreground images features helps to make high visual energy.

Database Feature Match : Extracted features will get compared with the database features of images.

Classifier: Classify the class of newly uploaded image using KNN classifier.

Policy Compare: Then use Linear matching technique to compare policy from the database.

A3P Engine: A3P(Adaptive Privacy Policy Prediction) engine will define accurate policies for user uploaded images. User will accept the policy otherwise revised for new policy.

4. CONCLUSION

In this paper, we plan a Saliency based approach which will help us to classify the input images more accurately there by improving the overall performance of the system. . This system will be useful in Facebook while image upload, automatic policy generation can be demonstrated, on social sites, while commenting/posting policy changes can be made in real time. 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. This system also assists Excellent Privacy Preference finding facility, Policy Recommendation System, Easy to use, Excellent security policies, Modify/accept privacy policies.

REFERENCES

[1] A. Besmer, H. Lipford, “Tagged photos: Concerns, perceptions, and protections,” in Proc. 27th Int. Conf. Extended AbstractsHuman Factors Comput. Syst., 2009, pp. 4585–4590.

[2] J. Bonneau, J. Anderson, and L. Church, “Privacy suites: for social networks,” in Proc. Symp. Usable Privacy Security, 2009.

[3] A. Kapadia, F. Adu-Oppong, C. K. Gardiner, and P. P. Tsang, “Social circles: Tackling privacy in social networks,” in Proc. Symp. Sable Privacy Security, 2008.

[4] Ghazinour, Stan Matwin and Marina Sokolova, “Yourprivacyprotector: A Recommender System For Privacy Settings In Social Networks”, International Journal of Security, Privacy and Trust Management (IJSPTM) Vol 2, No 4, August 2013.

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

[6] Alessandra Kristen LeFevre and Eytan Adar, The PViz Comprehension Tool for Social Network Privacy Settings, Tech. rep., University of Michigan, 2011.

[7] Peter F. Klemperer, Yuan Liang, L. Mazurek, “Tag, You Can See It! Using Tags for Access Control in Photo Sharing”, Conference on Human Factors in Computing Systems, May 2012.

[8] Sergej Zerr, Siersdorfer, Jonathon Hare, Elena Demidova , I Know What You Did Last Summer!:Privacy-Aware Image Classification and Search , Proceedings of the 35th international ACM SIGIR conference on Research and development in information retrieval, 2012.