Proposed Scheme for Privacy Policy Prediction of User Uploaded Images on Social Sites

[1]Somnath Mali, [2]Tushar Kulkarni, [3]Bharat Nirmal, [4]Prof. Dinesh B. Satre
[1,2,3,4] Marathwada Mitra Mandal Institute of Technology, Lohgaon, Pune

***Abstract*— Content sharing sites are very useful in sharing information and images but with the increasing demand of content sharing sites privacy and security concern have also increased. There is need to develop a tool for controlling user access to their shared content. So, we are developing an Adaptive Privacy Policy Prediction (A3P) system which will helpful for users to create privacy settings for their images. There is the two-level framework which assigns the best available privacy policy for the user's images according to user's available histories on the site.**

Index Terms— **Online information services, protection, security, web based service.**

I. INTRODUCTION

Content Sharing Sites are one of the most visited sites but they are still vulnerable. The proposed work is to provide some additional Privacy Policies that are used to enhance the existing Privacy Policies to images on Content sharing sites. Due to Content Sharing sites, each individual has opportunities to meet new people and friends in their own and also in the other diverse communities across the world. Users of Content Sharing services share an abundance of personal information with large number of friends connected all over the world. This improved technology leads to privacy violation where the users are sharing the large volumes of images across more number of peoples. Thus, in this paper creation of privacy policies is proposed where privacy of the user uploaded images is maintained to improve the user satisfaction level. The main objective of proposed system is to improve security of images on social sites which shares the personal information in the form of images to all the users connected across the world on social sites.

II. PREVIOUSLY WORK DONE

In this paper [1] the policy based infrastructure is proposed, with the help of a SNS designed in PHP that allows Users to express their privacy preferences with respect to who can access their data and for what purpose. Data provider support to enforce user privacy preferences, and supporting additional access models. In the paper [2], HSV based color space image retrieval method is proposed, based on the color distribution of the images and CBIR algorithm (Content base image retrieval).

In paper [3] Your Privacy Protector is proposed. Your Privacy Protector is a recommender system that shows how simple machine learning techniques may provide useful assistance in two tasks to Facebook users. In paper [4], the PViz policy comprehension tool is proposed. It is centered on a graphical display, which shows the users social network.

In paper [5] a survey has been conducted to discover whether social circles exist or not and whether these social circles would help users in social-networking application to set effective privacy policies. In paper [6], various Privacy policies for social networking sites have been discussed. Various privacy controls for social networking sites have also been proposed.

In paper [7], the concept of tagging and how it creates the access control policies is explained. In paper [8], the comprehensive review of various privacy policy approaches to improve the security of information shared in the social media sites have been proposed. The security and discuss further extensions on user image update and the compatibility with existing image sharing social functionalities is discussed in paper [9]. In paper [10] the concepts of user's awareness about the significant branches of their uploaded images have been discussed.

III. PROPOSED SYSTEM ARCHITECTURE

Following fig shows the application architecture of our system:

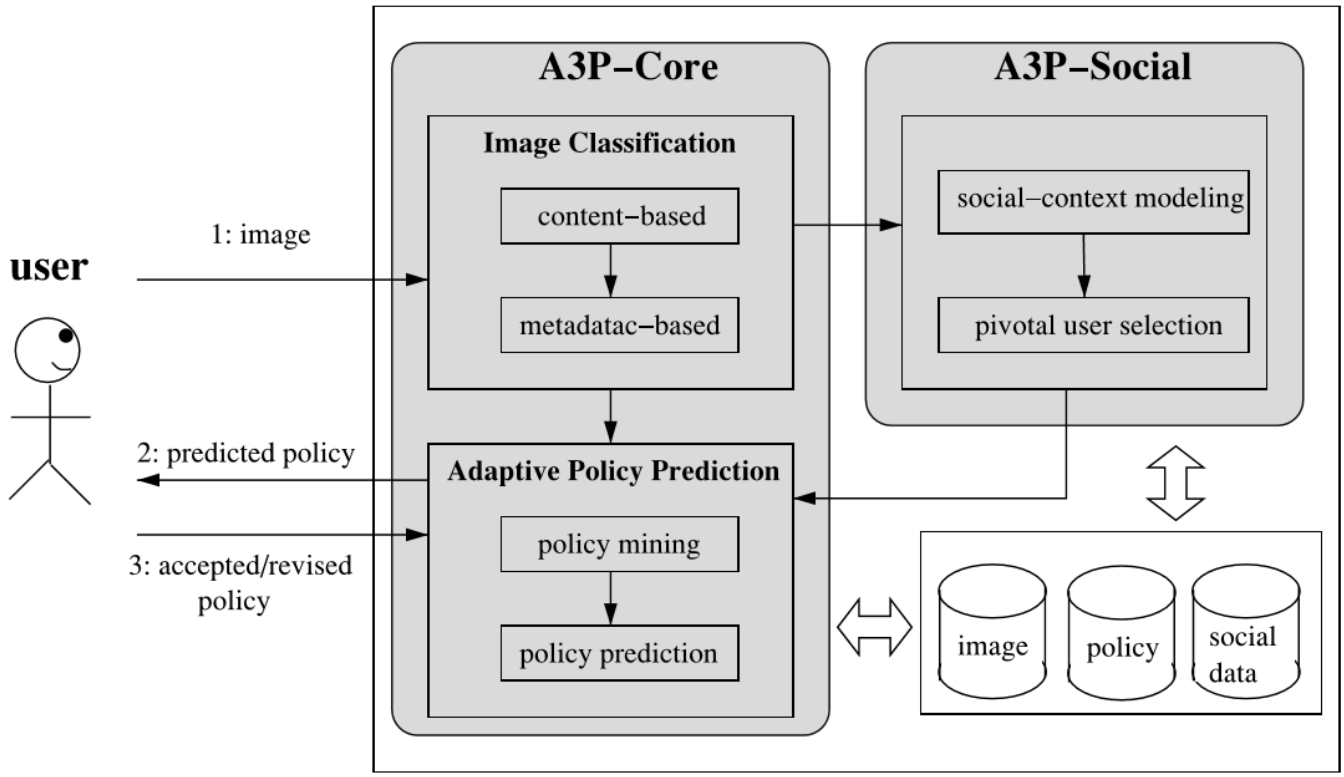

Fig 3.1 Application Architecture

Following is the explanation of proposed system architecture:

• 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 users community about their privacy practices along with users increase of content sharing activities.

In above cases, it would be beneficial to report to the user the latest privacy practice of content sharing sites that have similar background the user. The A3P-social groups users into content sharing sites with similar social context and privacy preferences, and continuously monitors the content sharing sites.

• When the A3P-social is invoked, it automatically identifies the social group for the user and sends back the information about the group to the A3P-core for policy prediction. At the end, the predicted policy will be displayed to the user.

• If the user is fully satisfied by the predicted policy, he or she can just accept it. Otherwise, the user can choose to revise the policy.

IV. TECHNIQUES USED

The proposed system has two main blocks. First is Image Classification and second is Adaptive Policy Prediction. Image Classification further has two parts Content based and Metadata based. When a new image is uploaded by the user the features of the image are calculated using three algorithms of CBIR (Content based Image Retrieval). The three algorithms are as follows: Color Extraction, Canny Edge Detection and Texture Detection. If the new image uploaded has tags associated with it then the image is classified under metadata based classification. Otherwise the image is classified under content based classification.

Once the image classification procedure is completed then policy prediction technique is carried out to define the policy for the new uploaded image. For this prediction technique Apriori Algorithm is used. Apriori is an algorithm for frequent item set mining and association rule learning over transactional databases. It proceeds by identifying the frequent individual items in the database and extending them to larger and larger item sets as long as those item sets appear sufficiently often in the database. The frequent item sets determined by Apriori can be used to determine association rules which highlight general trends in the database. Apriori has applications mainly in domains such as market basket analysis.

Association rule generation is usually split up into two separate steps:

1. First, minimum support is applied to find all *frequent itemsets* in a database.

2. Second, these frequent itemsets and the minimum confidence constraint are used to form rules.

Apriori uses breadth-first search and a tree structure to count candidate item sets efficiently. It generates candidate item sets of length k from item sets of length $k - 1$. Then it prunes the candidates which have an infrequent sub pattern. According to the downward closure lemma, the candidate set contains all frequent k-length item sets. After that, it scans the transaction database to determine frequent item sets among the candidates.

V. CONCLUSION

Content sharing sites are very useful in sharing information and images. More and more people go online and share their personal images using popular web services. But with the increasing demand of content sharing sites privacy and security concern have also increased. There is need to develop a tool for controlling user access to their shared content. So, an Adaptive Privacy Policy Prediction (A3P) system is proposed which is helpful for users to create privacy settings for their images. A two-level framework which assigns the best available privacy policy for the users images according to users available histories on the site is proposed in this paper. The proposed system automatically generates a policy for each newly uploaded image. The proposed system increases the security and privacy of social sites which in turn increases the satisfaction level of users.

REFERENCES

[1] A. S. Rathor, P. K. Mishra," Social Networking Websites and Image Privacy", IOSR Journal of Computer Engineering (IOSRJCE), May-Jun2013.

[2] S. Kaur, Dr. V. K. Banga," Content Based Image Retrieval: Survey and Comparison between RGB and HSV model", IEEE International Journal of Engineering Trends and Technology (IJETT), April2013.

[3] K. Ghazinour, S. Matwin and M. Sokolova,"Your privacy protector: A Recommender System For Privacy Settings In Social Networks", IEEE International Journal of Security, Privacy and Trust Management (IJSPTM), August 2013.

[4] Mazzia, K. Lefevre," The PViz comprehension tool for social network privacy settings", in Proc. Symp. Usable Privacy Security, 2012.

[5] A. Kapadia, F. Adu Oppong, C.K.Gardiner and P.P.Tsang,"Social circles: Tackling privacy in social networks ", in Proc.Symp.Usable Privacy Security, 2008

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

[7] P.Klemperer,Y.Liang,M.Mazurek,M.Sleeper,B.Ur,L.Bauer,L.F.Cranor,N.GuptaandM.Reiter,"Tag, you can see it!: Using tags for access control in photo sharing ", in Proc. ACM Annu. Conf. Human Factors Comput. Syst., 2012.

[8] A Survey on the Privacy Settings of User Data and Images on Content Sharing Sites", International Journal of Innovative Research in Computer and Communication Engineering, March2015.

[9] X.Yuan, X.Wang, C.Wang, A.Squicciarini and K.Ren,"Enabling Privacy preserving Image centric Social Discovery", 2014 IEEE 34th International Conference on Distributed Computing Systems, 2014.

[10] J. P. Pesce, D. L. Casas," Privacy Attacks in Social Media Using Photo TaggingNetworks: ACaseStudywithFacebook",2010.