Volume 6, Issue 10, October 2016 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Improving Privacy Accuracy for Shared Images over Social Networks by Using Privacy Risk Score Algorithm

K. N. Rajashekar*
M-Tech Student, Department of CSE
JNTUA College of Engineering, Ananthapuramu, India

Dr. K. F. Bharati
Assistant Professor, Department of CSE
JNTUA College of Engineering, Ananthapuramu, India

Abstract— Social media's have become one of the most important part of our daily life as it enables us to communicate with many people. Social Networking Sites like Google, Flickr and Facebook etc are providing more opportunities to meet the new people and also in the other diverse communities across the World. Users who are accessing the social-Networking services share their confidential Information with large number of Friends, which may leads to Privacy Violation. In the case of User's those who are sharing the most of image data across more number of People. So there is need to improve privacy according to the users Satisfactory Level. Existing System named Adaptive Privacy Policy Prediction (A3P) consists two –level Inter linkage Framework which monitors the user's available history in the sites, The A3P System helps the users by predicting privacy settings automaticallyfor the uploaded Images. The Adaptive Privacy policy Prediction system has comprehensive framework which infers privacy preferences based on information which is available for a given User. Improving the Privacy Prediction accuracy over the existing approaches is the main aim of the Proposed System. This system gathers most of the users data from the content image sharing sites and predicts policy prediction along with accessing restrictions along with the blocking schemes for the social networking sites by using the Data Mining Techniques. To perform this, the system utilizes APP (Accessing Policy Prediction) and Accessing Control Mechanism by applying the Privacy Risk Score (PRS) Algorithm.

Keywords— SIFT, AIA, KNN

I. INTRODUCTION

Social Networking is the important technology along with the hundreds of millions of people participating to view their content from media like audio, video, image and textetc. It assists an exterior of Self-Expression for the Users, also assists them for entertaining and for exchanging content with the other users by using Social Media E-Service .Social Networks like Facebook, Linked In, MySpace and Twitter have developed on the internet for the past Several Years. It provides a content sharing mechanism and connects People. Social Media are defined with a personal profile which can be modified as they wish. This feature is allowed by the Social Media, the users may contact with each other for their purposes like, Making Friendship, Business Sharing and for Sharing Knowledgeand Information. People are using Social Networks to get in touch with the known and unknown people, and to create, contribute the content which includes Personal Information, Videos, and Images. The service providers are providing facility for the users to collect the data and share them with Unauthorized Users. Avery familiar service provided in Social Networks is to produce the proposition in order to find events by using the Mutual Filtering Techniques. The success of the Social Networks is based on the users and cheering users to add more people to their circle and for sharing the data with other users in the social networks. By this the information will be spread across the World. End Users are nevertheless often not aware of the nature of spectators who access their data and sense of understanding created by organism among the Digital Friends. It often leads to the disclosures which may not be suitable in the Public Forum. Due to such open accessibility of the over exposed data in the Social Networks then the users will face Security and Privacy Risks.

II. LITERATURE SURVEY

In spite of fact that the content sharing will represent one of the most important features of the existing Social Networking Sites, Social Networks will not sustain any of the mechanism for the Collaborative Execution of the Privacy Settings for the Shared Content. [2] Social Networking sites are using by the huge number of users all over the world. Consider an example photo of a Student's 2016 graduation ceremony, for example it could be shared within the Flickr group or Google, which may unnecessarily expose that Student and leads to Privacy violations. Therefore many of the users have noticed the need for Privacy policy recommendation, which allows Users to configure the Privacy Settings easily and properly. Our work is related with existing recommendation system which employs Machine Learning Techniques. Chen et al. [7] proposed a System named Sheepdog which automatically inserts photos into suitable groups and recommends suitable tags to the Users on Social Media. They adopt the Concept Detection for predicting relevant concepts of a photo. Choudhury et al. [10] proposed a recommendation Framework for connecting the image content with communities in online Social Networking Media. They characterize the images through three steps: Visual Features,

Social Interaction and User generated text tagsfrom which they will recommend most likely groups for the given Image. The Semantic Retrieval of the images will be done by using a tool named Net for measuring SemanticComparison for annotating images in the Data Base. The Experimental Results make available enhanced retrieval performance when evaluated with Existing system.

III. PROBLEM STATEMENT

Maintaining privacy security has become a major problem, as demonstrated by the recent wave of publicized incidents, where the users share personal information inadvertently. In light of these incidents, there is a need of tools to help the users, having control access to their content shared is Apparent. Towards noticing this need, we need to propose an Adaptive Privacy Policy Prediction System, which helps the users to compose privacy policy settings for their Images. We analyze the role of social media context, metadata and image content as potential indicators of user's Privacy preferences. We propose a Two-Level Framework which is according to the user's availability of the history on the site which determines best available Privacy Policies for the user's images being uploaded.

IV. PROPOSED SYSTEM

4.1. A3P Framework:

Users can state their privacy policy needs about their content disclosures with their friends via the Privacy policy according to the Definition, 1. Definition 1 A is a Privacy policy of a user U which consists of following component: subject (S): A set of the users socially Connected to U. Action (A): A set of actions which were granted by U to S on D. Condition (C): A Boolean expression which has to satisfy in order to perform granted Actions. In the definition, users in S will be represented by their own identities, roles (e.g., coworkers, friends, family) or any organizations (e.g., profit organizations, non-profit organizations). D will be the set of images with in the users profile-Each image has its unique ID along with associated metadata.

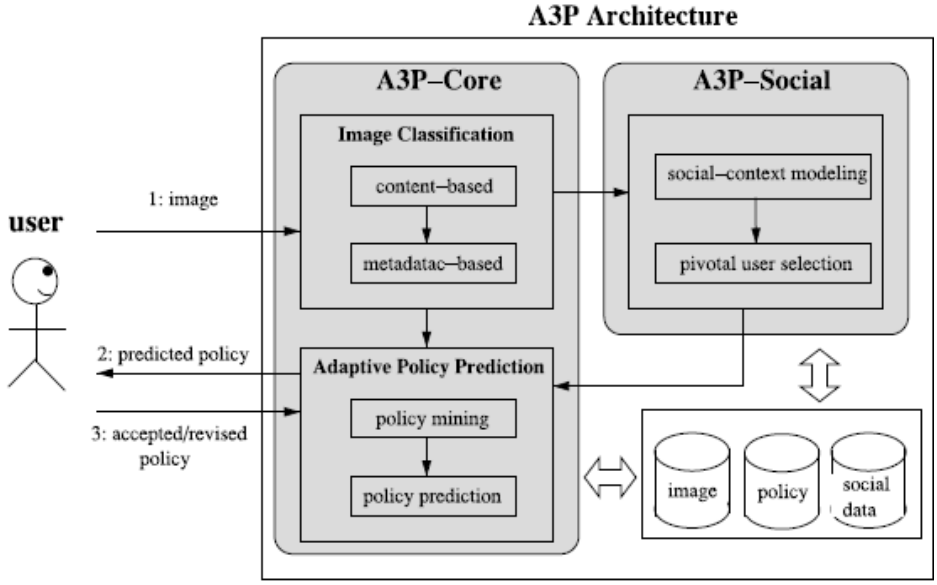


Fig1: Proposed framework

4.2. System Overview:

The A3P System has two major components: A3P-Core and A3P-Social. When an user uploads image, the image would be sent to the A3P core. The A3P Core will classify the image and it will determine if there is a need for invoking A3P Social. In the most of the cases, A3P-Core predicts Privacy policies to the users directly by based on their respective historical Behavior. If any of the following case is verified true then A3P-Core will invoke A3P-Social (i) If the user's may not have less enough image data for the type of images uploaded to conduct Policy Prediction; (ii) If the A3P-Core detects recent changes within the users about their privacy policy settings along with the users such as (new posts on one's profile, addition of friendsetc). The A3P-Social groups the users into the social communities with standardized privacy preferences and Social Groups. Whenever A3P-Social will getsinvoked, it Identifies automatically social groups for the users and sends back the information about the groups to the A3P-Core for predicting Policy Prediction. At the end the predicted privacy policy will be displayed to the Users.

4.3. Automated Annotation:

This system consists of two major tasks.One is Automatic Image Annotation and the other one is Annotation Based Image Retrieval. The Automatic Image Annotation phase will make use of manually training phase will make use of manually training sets taken to generate an Annotation Image. Annotation Based Images retrieval phase will gets a user query and then finds similar terms for query with the help of the Word Net. It also discovers the similarity between the matching Images. To annotate the images within the databases, features such as texture and color features will be extracted by using Color Histogram Methods.

4.3.1. Color Histogram Feature:

Color Histogram is the simplest and the most frequently used for representation of colors. The Color Histogram serves as an effective representation of the Data Content. A number of color spaces have been used such as LUV, RGB and HSV. Once the color space is specified, the color feature will be extracted by the regions or Images. An important color feature named Color Histogram is extracted. Color Histograms were frequently used for comparing Images. For this purpose the color image will be first converted into the grey level image, therefore the histogram values will be computed for the Grey Level Variations. According to the histogram values, the images were extracted from the Database.

4.4. SIFT Descriptors:

The SIFT based analysis will be involved in detecting salient locations within the images and extracts descriptors which are distinctive yet invariant to the changes in illumination, view point, etc. The standard SIFT (Histogram-Of Gradients) descriptor can be used. These 128 dimension descriptors will be thought of toughly as summarizing edge information in an image patches which will be centered at an Interest Point. We use the Clustering Algorithm for clustering a large collection of SIFT descriptors and will be labeled individually by local descriptor with the ID belongs to the closest cluster Centers.

4.4.1. Image Classification:

To obtain the group of images that are associated with the similar Privacy policy Preferences, We are proposing the Hierarchical optimized image based classification tool which classifies the image first will be based on their content's, it will refine independent categories into subcategories by based ontheir independent Metadata. Images which do not have Metadata will be grouped only by the content. Such a Hierarchical Classification gives higher priority for the image content and Minimize the influence of the Missing Tags.

4.4.1.1. Content-Based Classification:

The Content-Based optimization Classification Algorithm will compare image signatures and defines based on their quantified and sanitizing versions of Haar Wavelet transformation which will encodes the frequencies as well as spatial information which is related to the size, image, color, invariant transform, texture, shape, and symmetry etc. Then a small number of coefficients were selected in order to form signatures of the Image. The class of the posted Image is therefore it calculates as the class for the majority of M images Belongs. If predominant class is not found, then a new class will be created for the Image. Later on, if the system predicts Policy for this, the new image will turns out correct then the images will be inserted into the corresponding Images Category in the Image Database which helps to refine the Future Privacy Policy Prediction.

4.4.1.2. Metadata-Based Classification:

The Metadata-Based Classification will group the images into subcategories. This process is involved in three main steps. In the first step, it will extract the keywords from Metadata which will be associated with an image. The Metadata which is considered in our work are comments, tags, and captions. We identify all the verbs, nouns, and adjectives in Metadata and will store them as the Metadata Vectors. In the second step, we will select the hypernym with the highest frequency to be the representative Hypernym. The third step is to find the subcategory that an image belongs to. At the beginning, first the image forms a subcategory itself and then the representative hypernyms of the image becomes subcategories representative hypernyms. Then we can complete distance between representative hypernyms of the new incoming image and for the each individual Existing Subcategory.

4.5. Adaptive policy Prediction:

The adaptive Privacy policy Prediction Algorithm provides a predicted policy of the newly uploaded image to the user's reference. This prediction process consists of three main phases: (i) Policy normalization (ii) Policy Mining and (iii) policy Prediction.

4.5.1. Policy Normalization:

The Privacy Policy Normalization is a simple decomposition process which converts the users privacy policy into set of atomic rules in with which the Data (D) component is a single element Set.

4.5.2. Policy Mining:

We propose Hierarchical Mining Technique as an approach for policy mining. Our approach leverages an Association Rule Mining Technique inorder to discover the popular patterns in Policies. Policy Mining will be carried out within same category of the new image because the images in the same category are more likely under similar level of Privacy Policy Protection.

4.5.3. Policy Prediction:

The Policy Mining phase will generate several candidate privacy policies, while the goal of our system is to return most promising policy to the user. Thus, we present an approach for choosing the best candidate Policy which follows the user's privacy Tendency. To Model user's Privacy Tendency, we define a notion of the Strictness Level. Then policy Prediction will be done according to the user satisfactory level.

4.6. A3P-Social:

The A3P Social is employed by multi-criteria with Inference Mechanism, which generates the representative policies by the Leveraging Key information which is related to user's social context and his general attitude towards the Privacy Policy. A3P-Social gets invoked in two cases one is when the user is the new person (newbie) of a Site, and if he does not have enough images stored in the A3P-Core to infer the meaning and the customized Policies. The other case is when the system notices the prominent significant changes in the privacy trend in the user's social media circle.

4.6.1. Modeling Social Context:

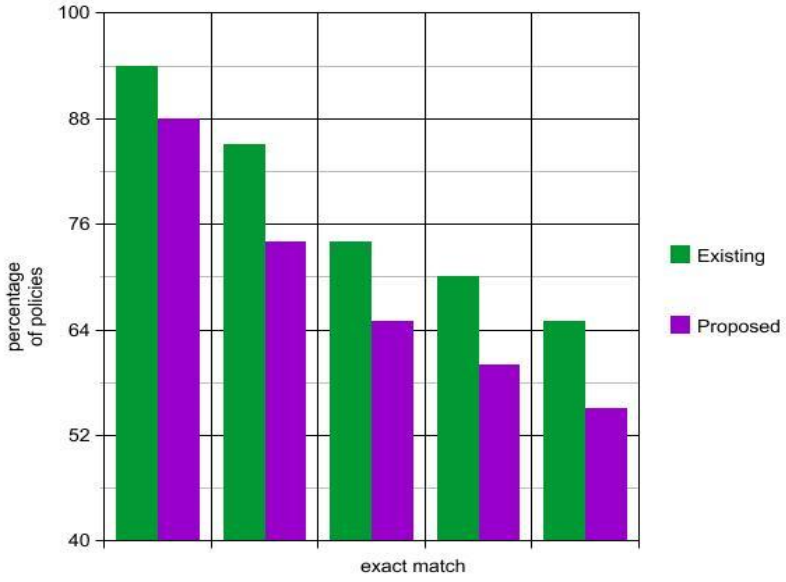
We can observe that the users with the similar background tends to have the similar privacy police concerns, as seen in the previous research studies and was also confirmed by our collected information. This observation inspired as to develop a Social Context Modeling Algorithm which can capture common social elements of the user's. Social Context Modeling Algorithm contains two major steps. The first step is to identify the image and then formalize the potentially important Factors. The second step is to group the users by based on the Identification Factor.

4.6.2. Identifying Social Group:

We introduce privacy recommendation process based on Social Groups obtained from previous Steps. We can search his/her attribute value in the inverted file and we can a obtain set of the candidate Social Groups. We can also count the number of occurrence of Candidate Groups during the Search. We select the Candidate Group with high occurrence of candidate Groups with high occurrence as the Social Group for the new User. We update social group information by including the new users as the Probation Members. The probation member will not be chosen by the A3P-Social Module until he/she upload sufficient images and will become a Regular Member.

V. EXPERIMENTAL RESULTS

The A3P System in combined with the AIA which is implemented by using Java. The proposed will be tested on our own Image Set. The Metadata based classification will compare the tags with the already uploaded Images. The system predicts privacy policy accordingly. In the Content- Based Classification, features of the image will be extracted by using the SIFT Algorithm. AIA will be done by using K-means and KNN Algorithm.



VI. CONCLUSION

We have projected an Adaptive Privacy Policy Prediction (A3P) scheme which helps the user's to computerize the Privacy Policy setting for their uploaded Images. The A3P Structure provides a wide-ranging structure to support Privacy Preferences based on the in order available for a given User's. we also successfully tackled the subject of the Cold-Start, leveraging Social Circumstance Information. Automatic Image Annotation will help's to overcome the issue of Metadata information of images being uploaded.

REFERENCES

[1] Anna Cinzia Squicciarini, Member, IEEE, Dan Lin, Smitha Sundareswaran, and Joshua Wede "Privacy Policy Inference of User-Uploaded Images on Content Sharing Sites" in IEEE transactions on knowledge and data engineering, vol. 27, no. 1, january 2015 193.

[2] R. Agrawal and R. Srikant,"Fast algorithms for mining association rules in large databases," in Proc. 20th Int. Conf. Very Large Data Bases, 1994, pp. 487–499.

[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, p. 357–366.

[4] M. Ames and M. Naaman, "Why we tag: Motivations for annotation in mobile and online media," in Proc. Conf. Human Factors Comput. Syst., 2007, pp. 971–980.

[5] A. Besmer and H. Lipford, "Tagged photos: Concerns, perceptions, and protections," in Proc. 27th Int. Conf. Extended Abstracts Human Factors Comput. Syst., 2009, pp. 4585–4590.

AUTHOR'S PROFILE

K.N.Rajashekar has obtained B. Tech degree inComputer Science and Engineering from Kottam College of Engineering A.P, India. Currently pursuing M.Tech in Computer Science from JNTUACEA Ananthapuramu.. E-mail: kn619shekar@gmail.com

Dr. K. F. Bharati is currently working as an Assistant Professor in the Department of Computer Science and Engineering in JNTUA College of Engineering Anathapuramu, A.P., India. She has receivedher Ph.D from JNTU Anatapur. She obtained her M.Tech from Visveswaraiah Technological University.

