IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 6, June 2016

Privacy Enhancement of User Data and Images on Content Sharing Sites

Gaikwad Swati Shankar[1], Prof. Amrit Priyadarshi [2]

PG Scholar, Department of Computer Engineering, DGOI, COE, Bhigwan, Savitribai Phule Pune University, India[1]

Assistant Professor, Dept of Computer Engineering, DGOI, COE, Bhigwan, Savitribai Phule Pune University, India[2]

Abstract: In today's world, sharing of personal information like images more easily due to the enhancement in content sites. Number of images user can share with more number of people. Increasing use of social media violates the privacy of contents due to large amount of sharing of the data. With the purpose to help the users to compose privacy settings for the images shared through social sites and improve content search method. This paper introduces a system called Adaptive Privacy Policy Prediction (A3P) system through which users can create their privacy settings for images and to satisfy other needs. The different contents like social context, image content, and metadata are administrated for users' privacy preferences. According to the history available on the site previously paper implement two level frameworks to provide a best privacy for the images which will be uploaded by the users. The images uploaded are classified according to the image categories and policy prediction algorithms on which our implementation depends and generates a particular strategy for user uploaded images and characteristic.

Keywords: Content sharing sites; Metadata; Privacy; Clustering; Cluster Labeling.

I. INTRODUCTION

Communication between the users now a day's emphasis on the images the readily established groups of users as the social networks along with the users not either communicated over social networks can communicate with each other, help each other, identify new groups and get a keen knowledge about their social surroundings. Hereby the images exposing any semantics may unknowingly pass any sensitive information. Taking an example in consideration if an employee posts his photograph of winning a best employee award on Picasa, it may lead to undesirable sharing information of his employee profile, family members and other personal information. Unwanted exposure of personal information and transgression may be caused due to sharing the images on the social network. The image owner information can be collected easily by any one which may lead to violation and data on the social media is persistent so undesirable exposure of the data.

II. RELATED WORK

The paper[1] established an A3P system. It automatically generates policies. Based on users personal features A3P system managed user uploaded images and images content and metadata Two components of A3P system are A3P Core and A3P Social. User uploaded image first sent to the A3P-core. Image classification is done. According to classification finding out a need for A3P-social.INaccurate classification and privacy violations occurred due to manual creation of metadata log data information. If not sufficient metadata information about image is available, then this method is inaccurate for generation of privacy policy. The paper[2] developed Privacy suites. This privacy suites created by experts, also by existing configuration UIs Users uses these suites to give privacy settings. Privacy suits are distributed to social sites using distribution channels. Verifying these suits by high level languages Transparency is maintained here. This language can't be able to understand by end users. The paper[3] uses different technologies like Social Circles Finders to secure the personal information of any user by implementing a web based solution from violation. It uses the policies of social networks to enhance the privacy setting of the user. This technology develops a friend's list of user; recognize their social networks and not showing them. The vital categorization of the friends list can be achieved by identifying the social network of subject and strength of their relationships. On the basis of the answers for the questions asked about their willingness to share their personal information the visual graphs of the users are clearly established. The paper[4] advised the appropriate privacy choices, these paper suggests system called as Your Privacy Protector which for these purpose grasps the privacy setting and colonial net behaviour of user personal profiles of the users are constructed using different attributes like personal profiles, client privacy settings on his photos collection and the client's interest areas. By analysing the user's profiles automatically privacy choices are assigned. Social profile can also display all the privacy setting of the user as orkut and can identify the possible threats to the profile. All needed settings are implemented to avoid those threats. The paper [5] proposed An interface is introduced by this paper called as PViz Comprehension Tool that represent how users design the group and particular privacy settings used on their social networks. Users can also point the problems faced during building the operative groups labels because they are permitted with transparency of their generated

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 6, June 2016

profile, further sub groupings at distinct levels of granularity. Compared with other tools this is more effective.

The paper [6] proposed during sharing in social network with every tag, system generates a control policy. Every photo tags are classified as organizational or communicative, this classification is done on basis of the subject's needs. Along with each tag every tagged photo is inculcated with the grids required for the access which can map with the users friends. Every individual involving himself can choose access information of his choice. Our results are the limitations to our study model on basis of the participants we assign and the photos they upload. Generated access control protocols are concerned by collection of the shortcomings. Some of the protocols and policies seem unfamiliar and random to the users because at the time of tagging, access control algorithm has no right over the elements information and also no interference into the policies implemented by the users. This makes policy tags permitted as "private" and "public". Ching-man Au Yeung propose a access control system based on a decentralized authentication protocol [7], data linked in social networks through similar web photos and other informational tags allotted to different photo sharing sites as facebook generates more conveying policies for the photos to shared and on the data provided by third party .

The paper [8] technique uses various categorization miniatures which works on the huge data collection with a particular privacy assigned through social commentary gaming. This technique advises privacy emphasis image search and examine private images. This categorisation enhance distension between natural and human-made objects on basis of image features like dimensions, margins, colours etc. which helps to promise presence or absence of particular object. This technique unites textual information of images with various features to provide security strategies.

III. OBJECTIVE OF STUDY

For some content sharing sites users can enter their privacy preferences itself. But users getting hard to set up and maintain this privacy settings. For large shared information this process become prosaic and error prone

Disadvantages Of Existing System**:**

- Users getting hard to set up and maintain privacy settings.
- Take more time for image searching.
- For large shared information this process become prosaic and error prone.
- Image sharing lead to unwanted disclosure and privacy violations.
- It only gives policy settings for traits. They may not be sufficient to address challenges brought by images for which privacy may vary substantially.
- Collected information can exploit security on the greater extent and unpredicted expose of one's social environment.

IV. PROPOSED SYSTEM

A. An Adaptive Privacy Policy Prediction (A3P) system is proposed in this paper which targets towards the trouble free privacy setting customisation for the users by developing various privacy policies.

- The limitations of all existing approaches are considerably removed by this approach where content based search is very fast.
- The lack of existing models in forensics analysis are not present the cluster, are divide based on similarity.
- This Approach is used for faster analysis of data.

B. The purpose of this project is to provide less number of page access to read or update operations using ranking and indexing technique, and hence is secure as well as time effective

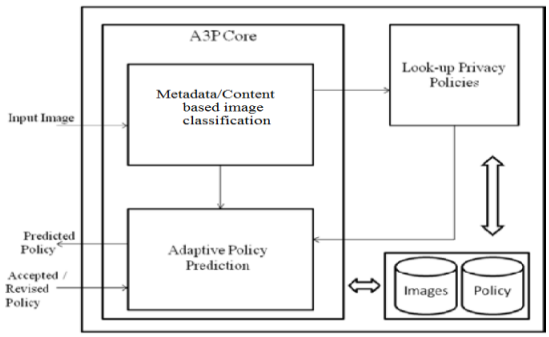

Fig. 1 Proposed System Architecture

Modules:

1. System Construction Module
2. Content-Based Classification
3. Metadata-Based Classification
4. Adaptive Policy Prediction

1. System Construction Module

Two main parts of A3P system are: A3P Core and A3P Social. Dataflow of architecture is, First uploaded image is send to the A3P Core. It categories image, finding out if necessary to invoke A3P social. According to documented behavior, A3P core directly predict the policies. Or it may invoke A3P Social for following situations: i) Required information to create policies is not providing for images ii) When it detects major changes in user community, increase in friend list, new post etc

2. Content-Based Classification

Images can be grouped according to their similar privacy preference. Hierarchical image classification technique is used. Hierarchical classification gives higher priority to image content and minimizes impact of tag missing. Image classification is depends on first their contents and then on metadata if it has. This model defines algorithm based on efficient, accurate similar image approach. Some images are included in multiple categories. This algorithm compares image signature. Similarity in contents defined by distance between image signatures.

DOI 10.17148/IJARCCE.2016.56153

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 6, June 2016

3. Metadata-Based Classification
This model classifies groups of images into subcategories under before said baseline categories. The model is consisting three steps. The metadata associated with an image. First step is extract keywords from metadata. Metadata is nothing but tags, captions and comments. Second step is to obtain hypernym(h) from each metadata vector. Third step is determining subcategory in which the image is residing. At the start the first image itself create subcategory, and its hypernym becomes the hypernym of image.

4. Adaptive Policy Prediction
For newly uploaded images the adaptive policy prediction algorithm provides a forecasting policy.
Changes to the user's privacy concerns are reflected by this policy. The prediction process consists of three phases, (a) policy normalization; (b) policy mining; and (c) policy prediction.

V. ALGORITHM

A. K-Means Algorithm:
1 Step 1:
Choose the number of clusters as 'k'.
2 Step 2:
Set the path of image dataset to cluster.
3 Step 3:
Randomly chose k images as centroids.
4 Step 4:
Calculate index or logical distance of each remaining image from centroids.
5 Step 5:
Assign the nearest image to corresponding centroids.
6 Step 6:
Repeat till number of iterations
Let 'i' denotes the image dataset.
1 'P' denotes the privacy setting.
2 'ip' denotes the input metadata or input image.
3 'o' denotes the output set.
4 If ip=metadata: Search i where filename=metadata
5 Fetch resulted 'o' set
6 If ip=image file:
Calculate RGB for image match RGB
7 Fetch resulted 'o' set
9 Check 'p' of result set 'o' for each file
10 Display image if 'p'=public or username=current username.

VI. RESULT ANALYSIS

FIG 2 POLICY RECOMENDED SYSTEM

This shows the recomendation of different policies to the users while uploading images.

Fig 3 Search Image

This shows the searching accurate images based on content or metadata.

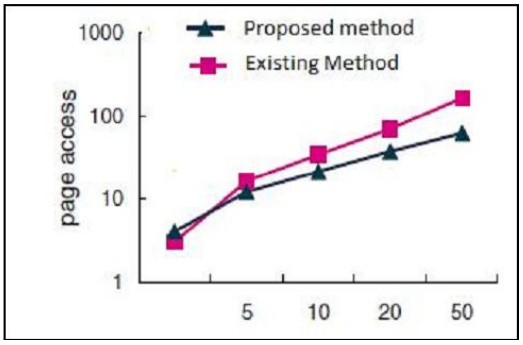

Fig.4 Difference between existing and proposed

The fig. Above shows the distension between the two systems proposed and existing system. Proposed system consists of limitations on the page access more when compared to the existing system.

VII. CONCLUSION

The proposed Adaptive Privacy Policy Prediction (A3P) system uses more generalized CBIR system which helps to increase the system searching ability and provide more accurate results. Clustering algorithm is used for image classification, is also done in absence of metadata.

The A3P system provides a complete framework and summarises privacy preferences on the basis of the information available for a given user. The system recommends privacy policies and help users for searching images efficiently with either metadata or contents of an image.

ACKNOWLEDGEMENT

I would like to thank all people who help me in different way. Especially, I am thankful to my guide and P.G. coordinator **Prof. Amrit Priyadarshi** for his continuous support and guidance in my work.
Also, I would like to thank H.O.D. of Computer Engineering Department, **Prof. S. S. Bere** for motivating me. Lastly, I thank to IJARCCE who have given opportunity to publish my paper.

REFERENCES

[1] Anna Cinzia Squicciarini, Member, IEEE, Dan Lin, Smith Sundareswaran, and Joshua Wede, "Privacy Policy Inference of User -Uploaded Images on Content Sharing Sites", IEEE Transactions on Knowledge and Data Engineering, Vol. 27, NO. 1, January 2015.

[2] J. Bonneau, J. Anderson, and L. Church, "Privacy suites: Shared privacy 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] Kambiz 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] Alessandra Mazzia Kristen LeFevre and Eytan Adar, The PViz Comprehension Tool for Social Network Privacy Settings, Tech. rep., University of Michigan, 2011.

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

[7] C. A. Yeung, L. Kagal, N. Gibbins, and N. Shadbolt, "Providing access control to online photo albums based on tags and linked data," in Proc. Soc. Semantic Web: Where Web 2.0 Meets Web 3.0 at the AAAI Symp., 2009, pp. 9–14.

[8] Sergej Zerr, Stefan 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.

[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.

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

[12] R. da Silva Torres and A. Falc~ao, "Content-based image retrieval: Theory and applications," Revista de Inform_atica Te_orica e Aplicada, vol. 2, no. 13, pp. 161–185, 2006.

DOI 10.17148/IJARCCE.2016.56153