AUTOMATIC PRIVACY PROTECTION OF USER UPLOADED IMAGES ON SOCIAL SITES

[1]B.Bhavani, [2]Dr. R. Jegadeesan [3]A.Pavithra, [4]R.Sai Spandana,[5]K.Srikanth, [6]B.UmaRani

[1,2,3,4]SB.Tech Final Year Students,[2,6]Associate professor-Department Of Computer Science And Engineering,

[1,2,3,4,5,6]Jyothishmathi Institute of Technology and Science, Karimnagar , India

Abstract : Online social networks like Face book and My space are popular. These sites have increased the number of people who connect and share their personal information such as photos and activities. This reveals that the privacy concerns of the people are rich and varied. Proper configuration of access control can be difficult and time-consuming .The user's lack of understanding of privacy settings can lead to a lack of willingness to set up privacy manually. We use a two-level framework that uses user history available on the site and sets the privacy policy for user images so that the user can easily use the policy setting and secure their images. In this, we use the Adaptive Privacy Policy (A3P) prediction system, which allows users to use the free privacy settings experience for unrest by automatically creating privacy policies.

***Index Terms* – Adaptive privacy policy prediction, social networking, online photo sharing, classification**

1.INTRODUCTION

More and more people go online today and share their personal images and get connected with people. Sharing of information takes place even in existing groups or social circles [1] .This helps people to get connected easily with each other. This connection helps to identify the new companions and gives an idea about their importance and social surroundings. Anyhow, content sensitive images may release personal information. Let us look at an example, where an image of a person in family event has to be uploaded in social site like Google+ circle or face book, but this image will be naked to everyone, rather than to only family members. This sharing of images in social sites may also lead to unnecessary exposure and privacy contravention [2] . In future, it is possible for other users to gather rich accumulated information can result in unnecessary disclosure of one's private environment and lead to misuse of one's private information.

Many of the content sharing sites concedes the users to drop their privacy specifications .But unexpectedly modern studies have shown that the users are trying very hard to set up the shared data can be wearisome and error-prone [5]. So the people have recognized the requirement of privacy recommendation system which can advice users to set their privacy with ease. Anyhow, current systems for setting privacy automatically appear to be insufficient to solve the unique privacy preferences of images [7], due to the amount of data intrinsically carried within the images and their dependency with the online environment wherein they are disclosed.

2. RELATED WORK

Our work is related to setting up privacy settings in social sites, recommendation systems, and privacy online image analysis.Many modern businesses have studied how to automate the task privacy settings .Bonneau et al [4] the concept of privacy groups was proposed which recommends that users have a set of privacy settings that the "experts" or other trusted friends have already set, so ordinary users can choose either direct setup or just need to make a slight adjustment. Similarly, Danizis [8] proposed an automatic learning approach extract privacy settings from the social context at home that the data is being produced.

In parallel with Deniz's work, Adu-Oppong et al. Develop privacy settings based on the concept of "social circles" consisting of groups of friends who are split by splitting friends' lists of users. Ravichandran et al. Studied how to predict user privacy preferences for location-based data based on location and time of day. Fang et al. Privacy Wizard suggested to help users to grant privileges to their friends. The wizard asks users to customize privacy first to your specific friends, then use this as an entry to create a workbook that classifies friends based on their profiles and automatically assigns privacy labels to friends not served. Recently, Klemperer et al .studied whether keywords and captions with users their image tags can be used to help users more intelligently create and maintain access control policies. Results corresponds to our approaches: tags created for the organization can be redirected for help in establishing reasonable access control rules. The above approaches focus on policy-making settings are for attributes only, so they are considered primarily social context like a buddy list. While interesting, they may not enough to meet the challenges posed by the image files that may vary significantly not only privacy because of the social context but also because of the actual image includes. As far as the images, the authors [7] presented in an expressive language for images uploaded to social sites. This work is complementary to us because we do not deal with it expression policy, but relying on the policy of common models.

Specification for our predictive algorithm . In addition, there is a wide range of work on analyzing the content of images, for classification and interpretation [6] And the arrangement of images also in the context of photo sharing sites such as Flickr . Among these works, Zier's work [9] may be the closest to our work. Zerr explores the perception of privacy images using a combination of features, both content and metadata. This is a binary classification (private versus generic), so the task of classification is very different from our classification.

3.SYSTEM OVERVIEW

The A3P system consists of two main components: A3P and A3P. The total data flow is the following. When a user loads an image, the image will be sent first to A3P. A3P classifies the image and determines whether there is a need to call social A3P. In most cases, A3P expects policies for users based directly on their historical behaviour . If one of the following conditions is validated A3P will call A3Psocial: (1) The user does not have sufficient data for the image type that is loaded to predict policies; (ii) The core A3P detects recent major changes between the user community regarding their privacy practices as well as increasing the activities of the user's social networks.

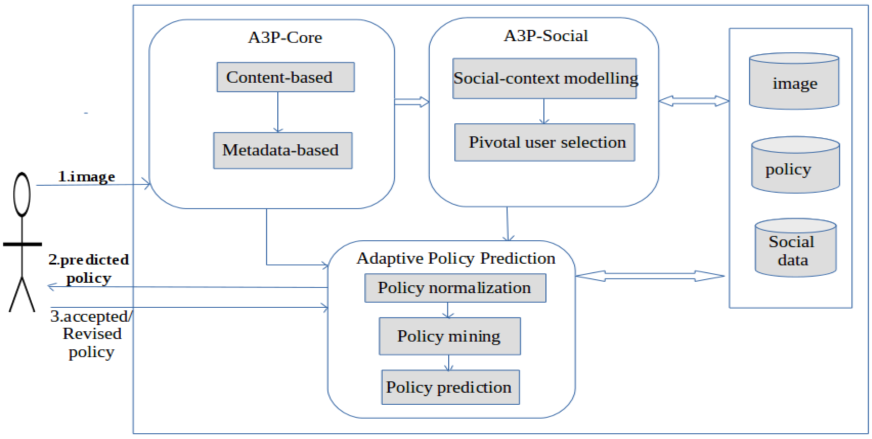

Fig 3.1: System Architecture

4.ADAPTIVE POLICY CORE

There are two main elements in A3P: (i) Image classification and (ii) adaptive policy forecasting. For user,his/her images are first categorized based on content and metadata. The privacy policies of each category of images are then analyzed to predict the policy.

4.1.IMAGE CLASSIFICATION

Content-based grouping:

For groups of images that may be associated with similar privacy preferences, we suggest a hierarchical image classification based on two indicators: 1) image content and 2) image metadata. In particular, we classify images first based on their contents, and then we improve each category into subcategories based on their metadata. Some images can be included in multiple categories as long as they contain the usual content attributes or metadata for those categories. In addition, images that do not contain metadata will be grouped only by content. This hierarchical classification gives higher priority to image content and reduces the impact of missing tags.

Metadata-based grouping:

Metadata-based classification aggregates images into subcategories within the above-mentioned base categories. The process consists of three main steps. The first step is to extract keywords from the initial data associated with the image. Metadata that is taken into account in our work are tags, comments, and comments. The second step is the derivation of hypnosis (referred to as h) of each vector of metadata. The third step is to find a subcategory to which the image belongs. This is a gradual procedure. Initially, the first image is a sub-category in itself and the Hypernms represent the image of the hypernyms of the sub-class representation.

4.2. ADAPTIVE POLICY FORECASTING

The policy prediction algorithm provides an expected policy for a user's newly uploaded image as a reference. More importantly, the expected policy will reflect potential changes to user privacy concerns. The forecasting process consists of three main phases: (i) normalization of policy; (ii) policy mining; and (iii) policy prediction.

Policy Mining

Our approach is to take advantage of mining techniques governing associations to discover popular patterns in policies. Policy mining is implemented within the same category of the new image because images in the same category are often under a similar level of privacy protection. The basic idea of pyramid mining is to follow a natural order in which the user determines a policy. Given the image, the user usually decides first who can access the image, then thinks about the specific access rights and the access conditions should eventually be improved, such as specifying the expiration date.

Policy Prediction

The mining stage in politics may generate several candidates, our system is to return more promising one for the user. As such, we offer a way to choose the best candidate policy that follows the user's privacy. To illustrate the direction of user privacy, we define the concept of rigor. The accuracy level is a quantitative measure that describes how to "narrow down" the policy.

5. A3P SOCIAL

A3P-social uses a multi-standard inference mechanism that generates representative policies using leverage. Basic information related to the user's social context Public attitude towards privacy. As mentioned before, A3Psocial will be called by the A3P core in two scenarios. One when a user is a beginner for a site, and does not You have enough images stored for the A3P-core to derive useful and customized policies. The other is when the system notices significant changes in the direction of privacy in the user's social circle, which may interest the user to adjust their privacy settings accordingly.

5.1. Social Context Modeling

Note that users who have a similar background tend to enjoy similar privacy fears, as seen in previous research studies also confirmed by our collection data. This observation inspires us to develop a social contextual modeling algorithm that can capture the social elements common to users and identify the communities they form users with privacy concerns. Then identified communities that have a rich set of images can serve as a basis for subsequent policy recommendations. The social context modeling algorithm consists of two main steps. The first step is to identify factors that are likely to be useful in your privacy settings. The second step is to group users based on specific factors.

5.2. Identifying Social Group

The process of policy recommendations based on social groups obtained from the previous step. Suppose a U user has uploaded a new image and recalled the A3P-core A3P-social recommendation for policy recommendation. A3P-social will find the most user-friendly social group U and then choose the representative user in the social group along with his image to be sent to the A3P-Core Policy Prediction Unit to create the recommended policy for user U.

6. RESULTS

The goal is to investigate whether the population is different, and the heterogeneous image set of the second data set affects the quality of the prediction. Also, this data set is characterized by better metadata, as the manual scan revealed that user-entered tags were fully completed, meaningful, and use keywords or stop words within them. For this experiment, we once again used the straw man's method of comparison which consists of the most recent replication of what was created user policy. This comparison is required to remove suspicion that mechanical telescope users may be completed mobilize the sources of tasks in an automated manner, without paying adequate attention to each individual task .We also tested quality achieved by A3P-core in case of only signs used, where previous experience showed that their marks is of little importance for the purpose of forecasting.

Results of A3P-core and A3P-social on Dataset:

Technique	Tag,Description download	View	Comment	Overall
A3P-core	90.52%	90.38%	90.38%	90.42%
A3P-social	84.45%	84.34%	86.56%	86.67%
Content-Based Classification	68.64%	66.12%	66.825%	66.84%
Metadata-Based Classification	86.64%	87.54%	87.03%	87.10%

TABLE 6.1: Results of A3P-Core and A3P-Social on Picalert Data Set

Major level in policy prediction:

In Table 6.2, all fixtures Common subjects and common actions are enumerated and set the integer value according to strict topics and corresponding acts. For example , the View action is more restrictive than the "tag" action. Given the policy, its value can be considered one of the value in table by matching its subject and work. If the policy contains multiple topics or actions and multiple results for values, we will look at the lowest one. Nothing is equal the table is created automatically by the system however can be adjusted by users according to their needs.

Top-Level	Theme	Action
0	Personal group1	View
1	Personal group2	Comment
2	Social group1	Tag,Comment
3	Social group 2	View,Download
4	New contact	View,Comment
5	Working group	Comment
6	Working group	Tag

TABLE 6.2: Major Level Look-Up Table

7.CONCLUSION

We have proposed a system consistent with the A3P privacy policy that helps users automate privacy policy settings for uploaded images. The A3P provides a comprehensive framework for deriving privacy preferences based on information available to a particular user. We also dealt effectively with the issue of cold start, and taking advantage of information on the social context. Our empirical study demonstrates that our A3P is a practical tool that offers significant improvements to current privacy practices.

REFERENCES

[1] A. C. Squicciarini, S. Sundareswaran, D. Lin, and J. Wede, “A3p:Adaptive policy prediction for shared images over popular content sharing sites,” in Proc. 22nd ACM Conf. Hypertext Hypermedia,2011, pp.261–270.

[2] Y. Liu, K. P. Gummadi, B. Krishnamurthy, and A. Mislove,“Analyzing facebook privacy settings: User expectations vs. reality,” in Proc. ACM SIGCOMM Conf. Internet Meas. Conf., 2011, pp. 61–70.

[3] P. Klemperer, Y. Liang, M. Mazurek, M. Sleeper, B. Ur, L. Bauer,L. F. Cranor, N. Gupta, and M. Reiter, “Tag, you can see it!: Using tags for access control in photo sharing,” in Proc. ACM Annu. Conf. Human Factors Comput. Syst., 2012, pp. 377–386.

[4] 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.

[5] K. Strater and H. Lipford, “Strategies and struggles with privacy in an online social networking community,” in Proc. Brit. Comput. Soc. Conf. Human-Comput. Interact., 2008, pp.111–119.

[6] A. Vailaya, A. Jain, and H. J. Zhang, (1998). On image classification: City images vs. landscapes. Pattern Recog. [Online]. 31(12),pp. 1921–1935. Available: http://www.sciencedirect.com/science/article/pii/S003132039800079X

[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] J. Yu, D. Joshi, and J. Luo, “Connecting people in photo-sharing sites by photo content and user annotations,” in Proc. IEEE Int.Conf. Multimedia Expo, 2009, pp.1464–1467.

[9] S. Zerr, S. Siersdorfer, J. Hare, and E. Demidova, “Privacy-aware image classification and search,” in Proc. 35th Int. ACM SIGIR Conf. Res. Develop. Inform. Retrieval, 2012, pp. 35–44

[10] S. Zerr, J. H. Stefan Siersdorfer, and E. Demidova, (2012). Picalert! data set. [Online]. Available: http://l3s.de/picalert/

[11] X. Su and T. M. Khoshgoftaar, “A survey of collaborative filtering techniques,” Adv. Artif. Intell., vol. 2009, p. 4, 2009.

[12]T. Jaeger, A. Edwards, and X. Zhang. (2003). “Policy management using access control spaces,” ACM Transactions on Information and System Security, 6(3):327–364

[13]H. Krasnova, O. Günther, S. Spiekermann, and K. Koroleva. (2009).“Privacy concerns and identity in online social networks,” Identity in the Information Society, 2:39–63.

[14]A.C.Squicciarini,D.Lin,S.Sundareswaran and J.Wede ,“Privacy Policy Inference of Multiple User-Uploaded Images on Content Sharing Sites”,in IEEE Transactions on Knowledge and Data Engineering,vol.27,no.1,pp.193-206,1 Jan.2015.

[15] H.Singh and M.Bhusry “Privacy policy inference of multiple user-uploaded images on social context websites(Automated generation of privacy policy),” 2017 3rd International Conference on Computational Intelligence & Communication Technology(CICT),Ghaziabad,2017,pp.1-5.

[16].Jegadeesan,R.,Sankar Ram M.Naveen Kumar JAN 2013 “Less Cost Any Routing With Energy Cost Optimization” International Journal of Advanced Research in Computer Networking,Wireless and Mobile Communications.Volume-No.1: Page no: Issue-No.1 Impact Factor = 1.5

[17]. Jegadeesan,R.,Sankar Ram, R.Janakiraman September-October 2013
“A Recent Approach to Organise Structured Data in Mobile Environment” R.Jegadeesan et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 4 (6) ,Page No. 848-852 ISSN: 0975-9646 Impact Factor:2.93

[18]. Jegadeesan,R., Sankar Ram October -2013 “ENROUTING TECHNICS USING DYNAMIC WIRELESS NETWORKS” International Journal of Asia Pacific Journal of Research Ph.D Research Scholar 1, Supervisor2, VOL -3 Page No: Print-ISSN-2320-5504 impact factor 0.433

[19]. Jegadeesan,R., Sankar Ram, M.S.Tharani (September-October, 2013)
”Enhancing File Security by Integrating Steganography Technique in Linux Kernel” Global journal of Engineering,Design & Technology G.J. E.D.T., Vol. 2(5): Page No:9-14 ISSN: 2319 – 7293

[20]. Ramesh,R., Vinoth Kumar,R., and Jegadeesan,R., January 2014
“NTH THIRD PARTY AUDITING FOR DATA INTEGRITY IN CLOUD” Asia Pacific Journal of Research Vol: I Issue XIII, ISSN: 2320-5504, E-ISSN-2347-4793 Vol: I Issue XIII, Page No: Impact Factor:0.433

[21]. Vijayalakshmi, Balika J Chelliah and Jegadeesan,R., February-2014
“SUODY-Preserving Privacy in Sharing Data with Multi-Vendor for Dynamic Groups“ Global journal of Engineering,Design & Technology. G.J. E.D.T.,Vol.3(1):43-47 (January-February, 2014) ISSN: 2319 –7293

[22]. Jegadeesan,R.,SankarRam,T.Karpagam March-2014 “Defending wireless network using Randomized Routing process” International Journal of Emerging Research in management and Technology

[23].Jegadeesan,R.,T.Karpagam, Dr.N.Sankar Ram , "Defending Wireless Network using Randomized Routing Process" International journal of Emerging Research in management and Technology ISSN: 2278-9359 (Volume-3, Issue-3) . March 2014

[24]. Jegadeesan,R., Sankar Ram "Defending Wireless Sensor Network using Randomized Routing "International Journal of Advanced Research in Computer Science and Software Engineering Volume 5, Issue 9, September 2015 ISSN: 2277 128X Page | 934-938

[25]. Jegadeesan,R., Sankar Ram,N. "Energy-Efficient Wireless Network Communication with Priority Packet Based QoS Scheduling", Asian Journal of Information Technology(AJIT) 15(8): 1396-1404,2016 ISSN: 1682-3915,Medwell Journal,2016 (Annexure-I updated Journal 2016)

[26]. Jegadeesan,R.,Sankar Ram,N. "Energy Consumption Power Aware Data Delivery in Wireless Network", Circuits and Systems, Scientific Research Publisher,2016 (Annexure-I updated Journal 2016)

[27]. Jegadeesan,R., Sankar Ram , and J.Abirmi "Implementing Online Driving License Renewal by Integration of Web Orchestration and Web Choreogrphy" International journal of Advanced Research trends in Engineering and Technology (IJARTET) ISSN:2394-3785 (Volume-5, Issue-1, January 2018

[28]. Pooja,S., Jegadeesan,R., Pavithra,S., and Mounikasri,A., "Identification of Fake Channel Characteristics using Auxiliary Receiver in Wireless Trnsmission" International journal for Scientific Research and Development (IJSRD) ISSN (Online):2321-0613 (Volume-6, Issue-1, Page No. 607-613, April 2018

[29]. Sangeetha,R., Jegadeesan,R., Ramya,P., and Vennila.,G "Health Monitoring System Using Internet of Things" International journal of Engineering Research and Advanced Technology (IJERAT) ISSN :2454-6135 (Volume-4, Issue-3, Page No. 607-613, March 2018.