ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

USER-UPLOADED IMAGES PRIVACY POLICY PREDICTION USING CLASSIFICATION AND POLICY MINING

Aishwarya Singh*, Sushmita Singh, Bhavesh Mandalkar
DYPIET Ambi, Pune

DOI: 10.5281/zenodo.47620

ABSTRACT

Social media become one of the most essential part of our daily life as it enables us to be in touch with a lot of people. Creation of social networking sites such as LinkedIn, Facebook and MySpace give opportunities to communicate new peoples and friends in their own and also in the other various communities across the world. Users of social media share plenty of personal information with a large number of "friends." These enhance technology leads to violations of privacy as the users are sharing the large volumes of images across more number of people. This privacy need to be concerned in order to improve the user satisfaction level. Toward addressing this need, an Adaptive Privacy Policy Prediction (A3P) system is provided to help users compose privacy settings for their images. The role of social context, image content, and metadata examine as possible indicator of user's privacy preferences. According to the user's available history on the social site, A3P system determines the best existing privacy policy for the user's images being uploaded. The result relies on an image classification structure for image categories which may be related to the same type of policies, and on a policy prediction algorithm for automatically generate a policy for each newly uploaded image, also according to the social features of the user. Our overarching goal is to provide better tools for managing privacy of information shared in the social media sites.

General Terms
Your general terms must be any term which can be used for general classification of the submitted material such as Pattern Recognition, Security, Algorithms et. al.

KEYWORDS: Social media; content sharing sites; Privacy; Meta data, A3P System.

INTRODUCTION

Online social networks are websites that permit users to build connections and interaction with other Internet users. Social networks store information remotely, instead of on a user's personal computer. Social networking can be used to communicate with friends, make new contacts and find people with analogous interests and ideas. The relation between privacy and a person's social network is complex. It is a necessary to develop more security mechanisms for different communication technologies, mainly for online social networks. Privacy is important to the design of security mechanisms. Most social network suppliers have offered privacy settings to allow or prevent others access to personal information details. In certain event users want information about them to be known only by a small circle of close friends, and not by strangers. In other instances, the user is ready to reveal personal information to unknown strangers, but not to those who know us better. Social network thinkers have discussed the importance of the relations of different depth and strength in a person's social network and the consequence of so-called weak binds in the flow of information across different nodes in a network.

A definition of internet, privacy would be the ability to control (1) what information user discloses about himself, and (2) who can access that information. Basically, when the data is collected or analyzed without the knowledge or permission of its owner, privacy is violated. For usage of the data, the owner of that data should be informed about the reason and objective for which the data are being or will be used. Most of the content sharing websites permit users to enter their privacy preferences. Unfortunately, recent studies have shown that users struggle hard to set up and maintain privacy settings [9], [10]. One of the main reasons provide is that given the amount of shared information this procedure can be monotonous and error-prone [11], [12].

Therefore, there is a need of policy recommendation systems which can help users to easily and properly configure privacy settings [2], [4], [13]. The privacy policy of user uploaded image can be provided based on the user social environment and historical behavior. Social context of users, such as their profile information and their relationships with others may give useful information about user's privacy preferences. The privacy policy of image uploaded by the user can be given based on the content of the image uploaded by the user and metadata. A hierarchical image classification which classifies images first based on their contents and then refines each category into subcategories based on their metadata. Images that don't contain metadata will be grouped only by their content. Such a hierarchical classification provides a higher priority to image content and minimizes the control of missing tags. A3P system contains two main building blocks: A3P-Social and A3P-Core. The A3P-core focus on examining each individual user's own image and metadata, while the A3P-Social suggest a community perspective of privacy setting probable for a user'sprospective privacy improvement. The interface between these building blocks is designed to equilibrium the benefits of meeting personal characteristics and getting community advice.

LITERATURE SURVEY

Sr no	Paper	Author	Privacy Methods Used	Merits	Demerits
1	Social circles: Tackling Privacy in social networks.	A. Kapadia, F. Adu-Oppong, C. K. Gardiner, and P. P. Tsang	Social Circles Finder	Transparency	Applicable to a limited set of users
2	Your privacy protect :A Recommender System For Privacy Settings in Social Networks	Kambiz Ghazinour, Stan Matwinand, Marina Sokolova	Your Privacy Protector	Transparency	Difficulty to understand
3	The P Viz Comprehension Tool for Social Network Privacy Settings	Alessandra Mazzia Kristen LeFevre and Eytan Adar	PViz Comprehension Tool	Ease of use	Less understandability for users
4	Privacy suites: Shared privacy for social networks	J. Bonneau, J. Anderson, and L. Church	Privacy suites	Transparency	Less understandability for users
5	Tag, You Can See It! Using Tags for Access Control in Photo Sharing	Peter F. Klemperer, Yuan Liang, Michelle L. Mazurek,	Tag based access control of data	Transparency	Applicable to a limited set of users
6	I Know What You Did Last Summer!: Privacy- Aware Image Classification and Search	Sergej Zerr, Stefan Siersdorfer	Privacy-Aware Image Classification and Search	Directly search for private data	Complexity
7	Decentralization: The future of online social networking	Ching-man Au Yeung	Tags and linked data	Applicable to multiple content sharing sites	Applicable to a limited set of users

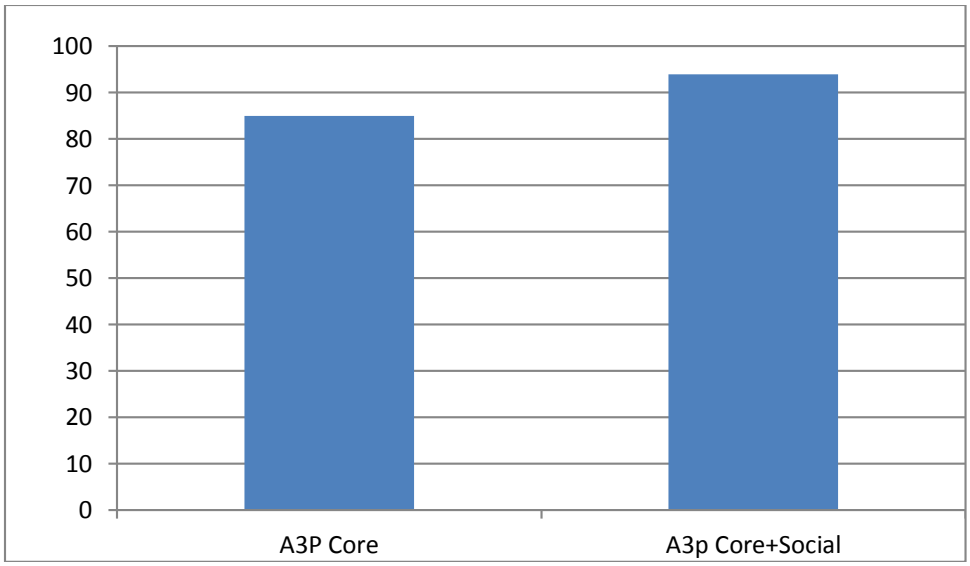
Fig 1: Table of Literature Survey

EXPERIMENTAL RESULT

Data Set

Image Type	Image colour	category	Subcategory	Image Group	Group name	Policy
JPG	Blue	Nature	River	3 images	G1	Friend, 6.jpg, view@Tag, 28-03-2017.
PNG	Red	Flower	Rose	6	G2	Family, 6.jpg, Download@Tag, 28-03-2017.
JPEG	Green	Nature	Grass	2	G1	Friend, 6.jpg, view@Tag, 26-11-2015.
GIF	Yellow	Flower	Rose	5	G2	Family, 6.jpg, Download@Tag, 24-11-2015.
JPG	Violet	Technic		4	G3	Co-Worker, 6.jpg, view@Download, 20-10 -2017.

Result



A3P Core	85
A3P Core +A3P Social	94

Fig 3: Table of result

SYSTEM ARCHITECTURE

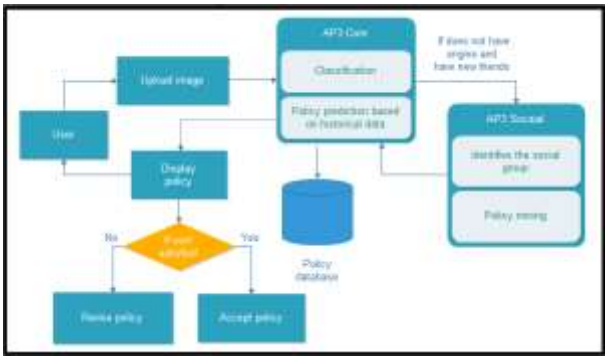


Fig 4: System overview

Upload Image

Image Type	Image Colour	Category	Subcategory
JPG	Blue	Nature	River

A3P Core

Image Classification:-

To find groups of images that may be linked to similar privacy preferences, we use hierarchical image classification which classifies images first according to their contents and then refine each category into subcategories based on their metadata.

Content Based Classification:-

The content-based classification is based on capabilities and yet perfect image similarity approach. This classification algorithm compares the signature of the image defined based on quantified and sanitized version of the Haar wavelet transform. For each image, the wavelet transform encodes frequency and information of spatial related to image color, shape, texture, symmetry, size etc. Then, a small number of coefficients are selected to form the signature of the image. The content relationship among images is then determined by the distance between their image signatures. Our selected relationship criteria include texture, symmetry, Shape. We also report for color and size. When a user uploads an image, it is held as an input query image. The signature of the newly uploaded image is balanced with the signatures of images in the current image database. For determining the group of the uploaded image, we find its first m nearby matches. The group of the uploaded image is then calculated as the group to which majority of them images belong. If no major group is found, a new group is formed in the image. Later on, if the predicted policy for this new image turns out correct, the image will be inserted into the related image category in our image database, to help refine future policy prediction.

Content Name	Image Group
Nature	1.jpg,2.jpg,3.jpg,6.jpg

Metadata Based Classification

The metadata-based classification form groups of image. The procedure consists of three main steps:- The first step is to extort keywords from the metadata related with an image. The metadata considered in this classification are tags, captions, and comments. The second step is to develop a representative hypernym (denoted as h) from each metadata vector. We first retrieve the hypernym for each tag in a metadata vector based on the Wordnet classification [39] and obtain a list of hypernym.. The third step is to find a subcategory that an image belongs to. This is an incremental process. At the beginning, the first image forms a subcategory as it and the representative Hypernyms of that image becomes the sub category's delegate Hypernyms. Then, we calculate the distance between delegate Hypernyms of a new incoming image and each existing subcategory.

Content Name	Subcategory Name	Image Group
Nature	River	1.jpg,3.jpg,6.jpg

Adaptive Policy Prediction

The policy prediction algorithms present a predicted policy of a newly uploaded image to the user for his/her suggestion. More importantly, the predicted policy will return the probable changes of a user's privacy concern. The prediction process contains three main phases:-

Policy normalization (ii) policy mining and (iii) policy prediction. The policy normalization is an easy breakdown process to convert a user policy into a set of atomic rules in which the data (D) component is a single-element set. The hierarchical mining approach for policy mining. In this use association rule mining techniques are used to determine popular model in policies. Policy mining is accepted out within the same category of the new image because images in the same category are more similar below the related level of privacy protection. The basic idea of the hierarchical mining is to track a natural order in which a user defines a policy.

The policy mining phase may produce several candidates' policies while the goal of our system is to return the most capable one for the user. Thus, we present an approach to select the best candidate policy that follows the user's privacy tendency. To model the user's privacy tendency, we define a concept of strictness level.

ijka	6.jpg	Friend, 6.jpg, view@Tag, 28-03-2017.

A3P Social:-

The A3P-social group users into social communities having related social context and A3P core invoke the A3P social, privacy preferences, and always examine the social groups. When the A3P-social is invoked, it routinely recognizes the social group for the user and then sends information about the group to the A3P-core for policy prediction. At the end, the predicted policy will be shown to the user. If the user is fully contained by the predicted policy, he or she can just accept it. Otherwise, the user can select to alter the policy. The actual policy will be collected in the policy repository of the system to predict the policy of future uploads.

Generate Social Group

The users with similar background be likely to have similar privacy concerns and also established by our collected data. These explanation encourage us to develop a social context modeling algorithm that can capture the common social elements of users and recognize communities produced by the users with similar privacy concern. The known

communities who have a rich set of images can then provide as the base of following policy recommendation. The social context modeling algorithm contain two main steps:

The first step is to recognize and make official potentially essential factors that may be useful of one's privacy settings. The second step is to group users based on the known factors. Besides basic elements in user's profile, many social sites also permit users to group their contacts based on relationships (e.g., friends, family members). If such grouping purposeful is available, we will consider its manage on privacy settings too. In a social site, some users may only have contact with their family members, while some users may have contacts including different kinds of people that they met offline or on the Internet. The distribution of contacts may discard light on the user's behavior of privacy settings. We assume that users who mainly share images among family members may not want to release personal information in public, while users having a large group of friends may be ready to share more images with a larger audience.

Example : Suppose that there are five users u1, u2, ..., u5 in social networking site. Each of them is related with five social context attributes: gender, hobbies, occupation, location and social connection.
u1: [Female, movie, accountant, NY, {0.6, 0.1, 0.2, 0.1}]
u2: [Female, movie, teacher, IL, {0.7, 0.1, 0.1, 0.1}]

u3: [Male, ski, student, CO, {0.3, 0.1, 0.5, 0.1}]
u4: [Male, ski, student, KS, {0.6, 0.15, 0.15, 0.1}]
u5: [Male, ski, student, MO, {0.2, 0.1, 0.6, 0.1}]
From the users' profile and social connection, two natural social groups can be formed.
G1 = {u1,u2}since they are both female who love movies and commonly share data with family members.
G2 = {u3, u4, u5}, since they are all male students who love sports.

Identifying Social Group:-
Example: Suppose that there are three social groups G1, G2, G3 which are formed based on the following frequent keywords.
G1: {female, movie, {0.6, 0.1, 0.2, 0.1}}
G2: {male, ski, student}
G3: {male, movie, IL }
We select the common attribute values except the social connection and build an inverted file as follows.
female: {G1}
IL: {G3}
hiking: {G3}
male: {G2, G3}
movie: {G1, G3}
student: {G2}

User Name	Group Name
ijka	G1

At the end, the predicted policy will be shown to the user. If the user is fully satisfied with the predicted policy, he or she can just accept it. Otherwise, the user can select to alter the policy. The actual policy will be stored in the policy repository of the system to predict policy of future uploads.

CONCLUSION

This paper express privacy policy technique for user's uploaded images in various social sites. Based on the user social behaviour and the user uploaded image the privacy policy can apply. A3P system is used, which provide users easy and properly, configured privacy setting for their uploaded image. By using this we can easily prevent unwanted

discloser and privacy violations. Unnecessary discloser may show the way to misuse of one's personal information .Users automate the setting of privacy policy for their uploaded images with the help of adaptive privacy policy prediction (A3P). Based on the information available for a given user the A3P system provides a comprehensive framework to infer privacy preferences. A3P system is a practical tool. An improvement over current approaches to privacy is offer by A3P.User can also select the people who can only see their image cannot comment on his image.

ACKNOWLEDGMENTS

It gives us great pleasure in presenting the preliminary project report on User-Uploaded Images Privacy Policy Prediction Using Classification and Policy Mining. I would like to take this opportunity to thank my internal guide Prof. Yogesh Pawar and project coordinator Prof. Sharmila Khurd, for giving me all the help and guidance I needed. I am really grateful to them for their kind support. Their valuable suggestions were very helpful. I am also grateful to Prof. Mangesh Manke, Head of Computer Engineering Department, Dr. D.Y Patil Institute of Engineering for his indispensable support, suggestions. In the end our special thanks to College Management and all Staff for providing various resources such as laboratory with all needed software platforms, continuous Internet connection, for Our Project.

REFERENCES

[1] Aishwarya Singh, Sushmita Singh, Bhavesh Mandalkar," User-Uploaded Images Privacy Policy Prediction UsinClassification and Policy Mining" , International Journal of Innovative Research in Computer and Communication Engineering(IJIRCCE) Vol. 3, Issue 8, August 2015.
[2] 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.
[3] Kambiz Ghazinour, Stan Matwin and Marina Sokolova, "Your privacy protector: A Recommender System for Privacy Settings in Social Networks", International Journal of Security, Privacy and Trust Management (IJSPTM) Vol 2, No 4, August 2013.
[4] Alessandra Mazzia Kristen LeFevre and Eytan Adar, The PViz Comprehension Tool for Social Network Privacy Settings, Tech. rep., University of Michigan, 2011.
[5] 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.
[6] 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.
[7] 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.
[8] Anna Cinzia Squicciarini, "Privacy Policy Inference of User-Uploaded Images on Content Sharing Sites", IEEE Transactions on Knowledge and Data Engineering, vol. 27, no. 1, January 2015.
[9] K. Strater and H. Lipford, "Strategies and struggles with privacy in an online social networking community," in Proc. Brit. Compute.
[10] Soc. Conf. Human-Compute. Interact, 2008, pp.111–119.
[11] R. Ravichandran, M. Benisch, P. Kelley, and N. Sadeh, "Capturing social networking privacy preferences," in Proc. Symp. Usable Privacy Security, 2009.
[12] 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, pp. 357–366.
[13] Mehmet Erkan Yüksel and Asım Sinan Yüksel, "An Application for Protecting Personal Information on Social Networking Websites", The Fourth International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies, 2010.
[14] J. Bonneau, J. Anderson, and L. Church, "Privacy suites: Shared privacy for social networks," in Proc. Symp. Usable Privacy Security, 2009.