ISSN 2395-695X (Print)
ISSN 2395-695X (Online)

International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)

Vol. 2, Special Issue 10, March 2016

MOBILE AUTHENTICATION OF USER-UPLOADED IMAGES

T.Krishnakaarthick (Assistant Professor), A.Bharathi, J.Elakiya, K.Gayathri, N.Ramya
Mail Id:krishnakumarbtech@gmail.com, bharathiinfotechit@gmail.com, anuelakiyainfotech@gmail.com
Gayunataraj03@gmail.com, nramyaselvamani@gmail.com
Nandha College Of Technology
InformationTechnology

ABSTRACT:

With the increasing volume of images users share through social sites, maintaining privacy has become a major problem, as demonstrated by a recent wave of publicized incidents where users inadvertently shared personal information. In light of these incidents, the need of tools to help users control access to their shared content is apparent. Toward addressing this need, a policy known as Adaptive Privacy Policy Prediction (A3P) system to help users has been used to compose privacy settings for their images. We examine the role of social context, image content, and metadata as possible indicators of users' privacy preferences. And also a two-level framework which according to the user's available history on the site, determines the best available privacy policy for the user's images being uploaded. It relies on an image classification framework for images categories which may be associated with similar policies, and on a prediction algorithm to automatically generate a policy for each newly uploaded image, also according to users' social features. And here a new one has been proposed which provides privacy for images even if someone tries to hack our images by knowing our password. It can be authenticated by sending information to the user as an One time password(OTP). Over time, the generated policies will follow the evolution of users' privacy attitude. We provide the results of our extensive evaluation over 5,000 policies, which demonstrate the effectiveness of our system, with prediction accuracies over 90 percent

INTRODUCTION:

Most content sharing websites allow users to enter their privacy preferences. Unfortunately, recent studies have shown that users struggle to set up and maintain such privacy settings. One of the main reasons provided is that given the amount of shared information this process can be tedious and error-prone. Therefore, many have acknowledged the need of policy recommendation systems which can assist users to easily and properly configure privacy settings. However, existing proposals for

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)

International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)

Vol. 2, Special Issue 10, March 2016

automating privacy settings appear to be inadequate to address the unique privacy needs of images due to the amount of information implicitly carried within images, and their relationship with the online environment wherein they are exposed.

In Adaptive Privacy Policy Pre-diction (A3P) system which provides users a hassle free privacy settings experience by automatically generating personalized policies. The A3P system handles user uploaded images, and factors in the following criteria that influence one's privacy settings of images: The impact of social environment and personal characteristics. Social context of users, such as their profile information and relationships with others may provide useful information regarding users' privacy preferences. For example, users interested in photography may like to share their photos with other amateur photographers. Users who have several family mem-bers among their social contacts may share with them pictures related to family events. However, using common policies across all users or across users with similar traits may be too simplistic and not satisfy individual preferences. Users may have drastically different opinions even on the same type of images. For example, a privacy adverse person may be willing to share all his personal images while a more conser-vative person may just want to share personal images

EXISTING SYSTEM:

Most content sharing websites allow users to enter their privacy preferences. Unfortunately, recent studies have shown that users struggle to set up and maintain such privacy settings.One of the main reasons provided is that given the amount of shared information this process can be tedious and error-prone. Therefore, many have acknowledged the need of policy recommendation systems which can assist users to easily and properly configure privacy settings.

DISADVANTAGES OF EXISTING SYSTEM:

Sharing images within online content sharing sites,therefore,may quickly lead to unwanted disclosure and privacy violations.

Further, the persistent nature of online media makes it possible for other users to collect rich aggregated information about the owner of the published content and the subjects in the published content.

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)

International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)

Vol. 2, Special Issue 10, March 2016

The aggregated information can result in unexpected exposure of one's social environment and lead to abuse of one's personal information.

PROPOSED SYSTEM:

In this paper, we propose an Adaptive Privacy Policy Prediction (A3P) system which aims to provide users a hassle free privacy settings experience by automatically generating personalized policies. The A3P system handles user uploaded images, and factors in the following criteria that influence one's privacy settings of images:The impact of social environment and personal characteristics. Social context of users, such as their profile information and relationships with others may provide useful information regarding users' privacy preferences. For example, users interested in photography may like to share their photos with other amateur photographers.The role of image's content and metadata. In general, similar images often incur similar privacy preferences, especially when people appear in the images. For example, one may upload several photos of his kids and specify that only his family members are allowed to see these photos.If the third person enters into our account the users are provided with one time password(otp).In this case account can be accessed only if they feed the correct otp which is been generated personally.That particular otp is obtained from the mobile number that's is given by the user already.

ADVANTAGES OF PROPOSED SYSTEM:

The A3P-core focuses on analyzing each individual user's own images and metadata, while the A3P-Social offers a community perspective of privacy setting recommendations for a user's potential privacy improvement. We design the interaction flows between the two building blocks to balance the benefits from meeting personal characteristics and obtaining community advice.

MODULES:

- System Construction Module
- Content-Based Classification
- Metadata-Based Classification
- Adaptive Policy Prediction

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)

International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)

Vol. 2, Special Issue 10, March 2016

- Authentication module

MODULES DESCSRIPTION:

System Construction Module

The A3P system consists of two main components: A3P-core and A3P-social. The overall data flow is the following. 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 user's community about their privacy practices along with user's increase of social networking activities (addition of new friends, new posts on one's profile etc).

Content-Based Classification

To obtain groups of images that may be associated with similar privacy preferences, we propose a hierarchical image classification which classifies images first based on their contents and then refine each category into subcategories based on their metadata. Images that do not have metadata will be grouped only by content. Such a hierarchical classification gives a higher priority to image content and minimizes the influence of missing tags. Note that it is possible that some images are included in multiple categories as long as they contain the typical content features or metadata of those categories.

Our approach to content-based classification is based on an efficient and yet accurate image similarity approach. Specifically, our classification algorithm compares image signatures defined based on quantified and sanitized version of Haar wavelet transformation. For each image, the wavelet transform encodes frequency and spatial information related to image color, size, invariant transform, shape, texture, symmetry, etc. Then, a small number of coefficients are selected to form the signature of the image. The content similarity among images is then determined by the distance among their image signatures.

Metadata-Based Classification

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)

International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)

Vol. 2, Special Issue 10, March 2016

The metadata-based classification groups images into subcategories under a fore mentioned baseline categories. The process consists of three main steps. The first step is to extract keywords from the metadata associated with an image. The metadata considered in our work are tags, captions, and comments. The second step is to derive a representative hypernym (denoted as h) from each metadata vector. The third step is to find a subcategory that an image belongs to. This is an incremental procedure. At the beginning, the first image forms a subcategory as itself and the representative hypernyms of the image becomes the subcategory's representative hypernyms.

Adaptive Policy Prediction

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

Authentication Module

A **one-time password** (**OTP**) is a password that is valid for only one login session or transaction, on a computer system or other digital device. OTPs avoid a number of shortcomings that are associated with traditional (static) password-based authentication; a number of implementations also incorporate two factor authentication by ensuring that the one-time password requires access to *something a person has* (such as a small keyring fob device with the OTP calculator built into it, or a smartcard or specific cellphone) as well as *something a person knows* (such as a PIN).

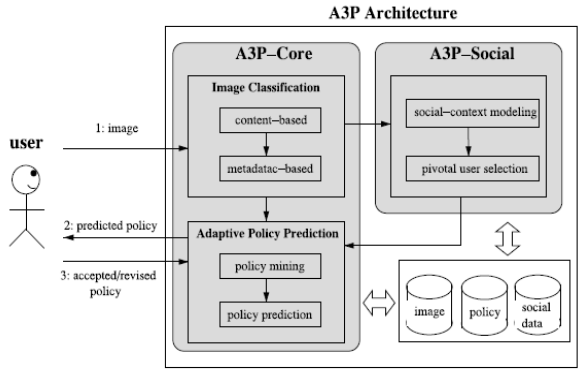
The most important advantage that is addressed by OTPs is that, in contrast to static passwords, they are not vulnerable to replay attacks. This means that a potential intruder who manages to record an OTP that was already used to log into a service or to conduct a transaction will not be able to abuse it, since it will no longer be valid. A second major advantage is that a user who uses the same (or similar) password for multiple systems, is not made vulnerable on all of them, if the password for one of these is gained by an attacker. A number of OTP systems also aim to ensure that a session cannot easily be intercepted or impersonated without knowledge of unpredictable data created during the *previous* session, thus reducing the attack surface further.

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)

International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)

Vol. 2, Special Issue 10, March 2016

SYSTEM ARCHITECTURE:



TheA3Psystemconsistsoftwomaincomponents:A3P-core and A3P-social. The overall data flow is the following. Whenauseruploadsanimage,theimagewillbefirstsent to the A3P-core. The A3P-core classifies the image and determineswhetherthereisaneedtoinvoketheA3P-social. In most cases, the A3P-core predicts policies for the users directlybasedontheirhistoricalbehavior.Ifoneofthefol-lowingtwocasesisverifiedtrue,A3P-corewillinvokeA3P- social: (i) The user does not have enough data for thetype oftheuploadedimagetoconductpolicyprediction;(ii)The A3P-coredetectstherecentmajorchangesamongtheuser's communityabouttheirprivacypracticesalongwithuser's increase of social networking activities (addition of new friends, new posts on one's profile etc). In above cases,it would be beneficial to report to the user the latest privacy practiceofsocialcommunitiesthathavesimilarbackground astheuser.TheA3P-socialgroupsusersintosocialcommu- nities with similar social context and privacy preferences, and continuously monitors the social groups. When the A3P-socialisinvoked,itautomaticallyidentifiesthesocial groupfortheuserandsendsbacktheinformationaboutthe grouptotheA3P-coreforpolicyprediction.Attheend,the predictedpolicywillbedisplayedtotheuser.Iftheuseris fully satisfied by the predicted

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)

International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)

Vol. 2, Special Issue 10, March 2016

policy, he or she can just acceptit.Otherwise,theusercanchoosetorevisethepolicy. The actual policy will be stored in the policy repositoryof thesystemforthepolicypredictionoffutureuploads.

A3P-SOCIAL:

The A3P social employs a multi-criteria inference mechanism that generates representative policies by leveragingkey information related to the user's social context and his general attitude toward privacy. As mentioned earlier, A3P- social will be invoked by the A3P-core in two scenarios. One is when the user is a newbie of a site, and does not have enough images stored for the A3P-core to infer mean- ingful and customized policies. The other is when the system notices significant changes of privacy trend inthe social context, it rarely happens that users share the same values of all social context attributes. More commoncases are that a group of users have common values for asubset ofsocialcontextattributes.Suchsubsetcanbedifferentfor differentgroupsofusers,whichmakestheusergroupinga challengingtask.Weillustratethescenariousingthefollowingexample.Forsimplicityofillustration,wetakeasmaller setofattributestobeconsidered. Suppose that there are five users u_1, u_2, ..., u_5 in a social networking site. Each of them is associated with five social context attributes: gender, hobbies, occupa-tion, location and social connection.

u_1: [Female, movie, accountant, NY, {0.6, 0.1, 0.2, 0.1}] u_2: [Female, movie, teacher, IL, {0.7, 0.1, 0.1, 0.1}]u_3: [Male, ski, student, CO, {0.3, 0.1, 0.5, 0.1}] u_4: [Male, ski, student, KS, {0.6, 0.15, 0.15, 0.1}] u_5: [Male, ski, student, MO, {0.2, 0.1, 0.6, 0.1}]

From the users' profile and social connection, two nat-ural social groups can be formed.

G_1 = fu_1; u_2g, since they are both female who love movies and frequently share data with family members.

G_2 = fu_3; u_4; u_5g, since they are all male students who love sports.

In the above example, we observe that the first social group is formed based on attributes: gender, hobbies and social connection, while the second social group is formed based on a different set of attributes which are gender, hob-bies and occupation. To identify such dynamic social groups, we

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)

International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)

Vol. 2, Special Issue 10, March 2016

employ an a priori [2]-based data mining Algo-rithm. Unlike the original a priori which requires exact matches of items in different transactions, we allow a fuzzy mapping. This is important for matching the social connec-tion attribute which would be just slightly different in the same social group as shown in Example 7. Therefore, we define the matching of social connection attribute as the val-ues of this attribute within a small threshold. Definition 2 describes the social groups extracted by our algorithm.

Au**thentication Module**

A **one-time password** (**OTP**) is a password that is valid for only one login session or transaction, on a computer system or other digital device. OTPs avoid a number of shortcomings that are associated with traditional (static) password-based authentication; a number of implementations also incorporate two factor authentication by ensuring that the one-time password requires access to *something a person has* (such as a small keyring fob device with the OTP calculator built into it, or a smartcard or specific cellphone) as well as *something a person knows* (such as a PIN).

The most important advantage that is addressed by OTPs is that, in contrast to static passwords, they are not vulnerable to replay attacks. This means that a potential intruder who manages to record an OTP that was already used to log into a service or to conduct a transaction will not be able to abuse it, since it will no longer be valid. A second major advantage is that a user who uses the same (or similar) password for multiple systems, is not made vulnerable on all of them, if the password for one of these is gained by an attacker. A number of OTP systems also aim to ensure that a session cannot easily be intercepted or impersonated without knowledge of unpredictable data created during the *previous* session, thus reducing the attack surface.

CONCLUSION:

We have proposed an Adaptive Privacy Policy Prediction (A3P) system that helps users automate the privacypolicy settings for their uploaded images. The A3P system pro- videsacomprehensiveframeworktoinferprivacypreferen-cesbasedontheinformationavailableforagivenuser.We also effectively tackled the issue of cold-start, leveraging social context information. Our experimental studyproves that our A3P is a practical tool that offers significant improvementsovercurrentapproachestoprivacy.

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)

International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)

Vol. 2, Special Issue 10, March 2016

REFERENCE:

[1] A.Acquisti and R. Gross, "Imagined communities: Awareness, information sharing, and privacy on the facebook," in Proc. 6th Int. Conf. Privacy Enhancing Technol. Workshop, 2006,pp. 36–58.

[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, pp. 357–366.

[4] D. G. Altman and J. M. Bland ,"Multiple significance tests: The bonferroni method," Brit. Med. J., vol. 310, no. 6973, 1995.

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

[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.