ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

A Survey on an Approach to Adaptive Privacy Policy Presumption under Images on Content Sharing Sites

Shruthi G

M. Tech student, Dept of CSE, UBDT College of Engineering, Davanagere, Karnataka, India

ABSTRACT: It has increased the uploading and downloading rate of images and text as the social media has increased. Major problem is maintaining the privacy issues. The overall system is made busy with data sharing and post updating. Adaptive Privacy policy Prediction (A3P)is the proposed system, a dedicated technique of for user detection and sharing. The overall system is programmed to maintain the policies of shared content. The system is simulated under JAVA IDE for understanding the real-time scenario of technique and challenges. The proposed system has successfully achieved the objective and the results are archived in the thesis.

KEYWORDS: Policy recommendation system, privacy setting, A3P, Social media, web based service, policy prediction

I.INTRODUCTION

Many websites allow sharing of photos, Web is very popular for sharing photos now a days.Therefore many users have recognized the need of policy recommendation systems which can accommodate users to properly configure privacy settings [2]. Most of web sharing sites provide access specifies that is whether a photo can be private, public or protected visible to their friends or those who are there family member. This setting can be applied by user to particular photo or a set of particular photos. Website tags are extensively used on photos. These tags are providing rich information about photos. So, using these, tags assigned to the photos a better access control mechanism can be provided that is rich images/photos reveal the sensitive information.Sharing websites allow users to enter their privacy preferences but users struggle to maintain the privacy settings. So this results in unvarying and errors. In this paper, an Adaptive Privacy Policy Prediction (A3P) system is used to provide users privacy settings easily by automatically generating personalized policies. This system handles user uploaded images.

System overview:

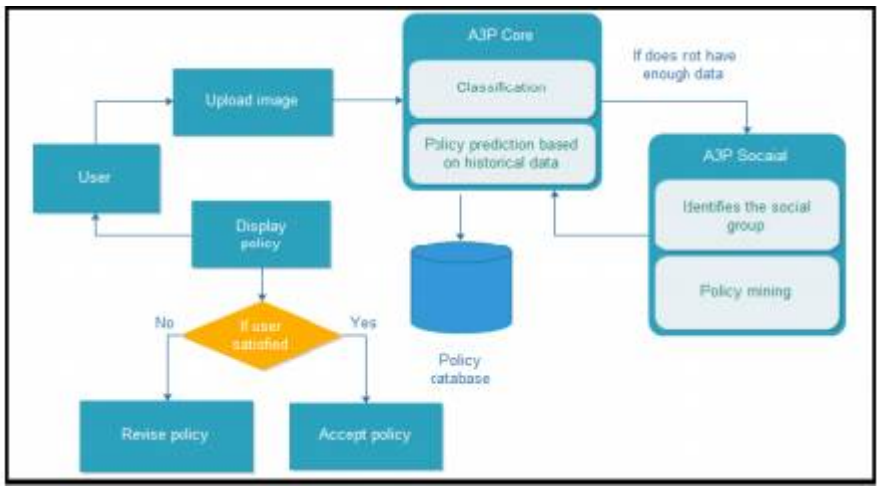

Fig1.System overview

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

A3P Core and A3P Social are the two important building blocks.A3P Core contains classification and historical data on policy prediction. A3P Social contains identification of social circles and mining. First user uploads the image and it goes through A3P Core which classifies and policy is determined.The A3P-social automatically determines social group of users .After that it sends back group information to the A3P-core for policy prediction. After policy prediction, predicted policy will displayed to user. If user satisfies they can accept that policy otherwise he can revise the policy. The actual policy will be store in repository for future image uploads [1].

II. RELATED WORK

2.1 Privacy Setting Configuration

Bonneauet proposed the privacy concept which suggest to users to set a privacy setting "expert" users or other trusted friends have already set, so that normal users can either directly choose a setting or only need to do minor modification. Danezis[12] proposed a machine-learning based approach to automatically extract privacy settings from the social context within which the data is produced. Adu-Oppong et develop privacy settings based on a concept of "Social Circles" which consist of clusters of friends formed by partitioning users' friend lists. Ravichandran et studied how to predict a user's privacy preferences for location-based data (i.e., share her location or not) based on location and time of day. Klemperer et al studied whether the keywords and captions with which users tag their photos can be used to help users more intuitively create and maintain access-control policies. The approaches focus on deriving policy settings for only traits, so they mainly consider social context such as one's friend list. While interesting, they may not be sufficient to address challenges brought by image files for which privacy may vary substantially not just because of social context but also due to the actual image Content.Adaptive Privacy Policy Prediction (A3P) system, a free privacy settings system by automatically generating personalized policies. The A3P system handles user uploaded images based on the person's personal characteristics and images content and metadata in A3P Core and A3P Social.[6]

2.2 Recommended System

Chen et proposed a system named Dog to automatically insert photos into appropriate groups and recommend suitable tags for users on Flickr. They adopt concept detection to predict relevant concepts (tags) of a photo. Choudhury proposed a recommendation framework to connect image content with communities in online social media. They characterize images through three types of features: visual features, user generated text tags, and social interaction, from which they recommend the most likely groups for a given image. Four common types of actions: view, comment, tag, download.Online social networking users communities are revealing huge number of personal information, facing the variety of risks. Our ongoing research investigates mechanisms for socially appropriate privacy Management in online social networking communities. We are examining the role of interface usability in current privacy settings as a role first. Here a view of profile information significantly improved the understanding of privacy settings. [5]

III. PROPOSED ALGORITHM

Proposed system is designed for maintaining the policy privacy updates and accessing content which is shared in social media. Proposed system purpose is to retrieve an effective approach for privacy preserving and content sharing.On appending this system to the real time environment, the efficiency and reliability of the OSN network can be improved.We present an A3P framework Adaptive Privacy Policy Prediction that means to provide clients a trouble free security settings encounter the experience via consequently creating modifying strategies. The framework A3P handles client transference pictures, and figures the appearing criteria that which influences one's own security settings of images: The effect of social context and individual attributes. Social setting of clients, for example, their profile data and links with others might give useful data in considering to user's security inclinations. For example, clients have enthusiasm on photography may get a kick out of communicate their photographs to other learner picture takers. The part of picture's substance and metadata. By and large, similar pictures frequently bring about comparable shield inclinations, especially when individuals show up in the pictures. For instance, one person may transport a few photographs of his children and specify that lone his relatives are given permission to view his specified photographs.

3.1 Algorithm

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

STEP1. Image collection under A3P techniques

STEP2. A3P Core architecture activation

```
While (true)
        For every Image acquired apply
                If(Image==contentbased)
                        Do
                        Image(true)
                        Set value to FALSE
                End If
                Else
                        Image(FALSE)
                        Set value to TRUE
                End Else
End While
```

On value (TRUE)

```
Fetch metadata objective values
```

End condition

STEP3. Data attribute & social media Analysis

```
On (value==TRUE
&&Image==contentbased)
Map
        Social graphical and algorithmic values
```

Fetch control to policy prediction 4.

STEP4. Data adaptive policy prediction

```
For all (Data==TRUE)
        Apply (policy) on Image
                If (policy)
                        TRUE::mining
```

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

FALSE::Exit

Fetch policy.

STEP5.Review policy & perceiving of Data/Images.

Detailed explanation of above algorithm for the fig1 as shown above. Firstly in step1 collection of images in A3P technics which mainly contains A3P core and A3P social. In step 2 activation A3P Core architecture, for every image in A3P core classification of particular image is done and also policy is predicted ,if image is content based fetch the meta data objective values. In step3 social media analysis is done if and only if the image is content based and map Social graphical and algorithmic values. In step 4 adaptive policy prediction data that is if data is true apply policy on image and fetch that policy and review policy & perceiving of Data/Images.

IV. CONCLUSIONS AND FUTURE WORK

We proposed an Adaptive Privacy Policy Prediction (A3P) system that helps users automatically generating privacy policy settings for their uploaded images. The A3P system provides a framework to conclude privacy on the information available for a given user. The model has been simulated under a JAVA background and thus the simulation of data security is highlighted and achieved. Under the proposed system, the aligned attributes are collected and the privacy of the active and unconnected users is monitored and thus the overall system is simulated under this respective environment.

The system can be moved and deployed under the cloud environment for faster and smoother accessing of data models. This model based interruption is increased and enhanced for the upcoming version.

REFERENCES

[1]R. Agrawal and R. Srikant,"Fast algorithms for mining association rules in large databases," in Proc. 20th Int. Conf. Very Large DataBases, 1994, pp. 487–499.
[2] R. Ravichandran, M. Benisch, P. Kelley, and N. Sadeh, "Capturing social networking privacy preferences," in Proc. Symp. Usable Privacy Security, 2009.
[3] 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.
[4] KambizGhazinour, 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.
[5] J. Yu, D. Joshi, and J. Luo, "Connecting people in photo-sharingsites by photo content and user annotations," in Proc. IEEE Int.Conf.Multimedia Expo, 2009, pp.1464–1467.
[6] A. Kapadia, F. Adu-Oppong, C. K. Gardiner, and P. P. Tsang, "Social circles: Tackling privacy in social networks," in Proc. Symp. Usable Privacy Security, 2008.
[7] 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.
[8]A. Singhal, "Modern information retrieval: A brief overview,"IEEE Data Eng. Bullet., Speicial Issue on Text Databases, vol. 24, no. 4, pp. 35-43, Dec. 2001.
[9] 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.
[10]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. 16thACM Int. Conf. Multimedia, 2008, pp. 737–740.
[11] L. Church, J. Anderson, J. Bonneau, and F. Stajano, "Privacy stories: Confidence on privacy behaviors through end user programming,"inProc. 5th Symp. Usable Privacy Security, 2009.
[12] J. Bonneau, J. Anderson, and G. Danezis, "Prying data out of a social network," in Proc. Int. Conf. Adv. Soc. Netw. Anal. Mining.,2009, pp.249–254.

BIOGRAPHY

Shruthi Gis a MTech post graduate student in computer science and engineering,UBDT college of engineering, Davanagere, Karnataka, India. She received her Bachelor of Engineering in computer science from STJIT, Ranebennur, Haveri dist. Karnataka,India in 2013.