IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Volume-4, Issue-4 E-ISSN: 2347-2693

An Adaptive Privacy Policy Prediction for Classifying the Images as Public and Private for Secured Transaction

Kavitha S[1]*. and H Girisha[2]
[1*,2] *Department of Computer science, VTU belgaum, India*

www.ijcseonline.org

Received: Mar/28/2016 Revised: Apr/07/2016 Accepted: Apr/22/2016 Published: Apr/30/2016

***Abstract*—**With the expanding volume of pictures clients offer through social locales, keeping up security has turned into a noteworthy issue, as exhibited by a late influx of advanced episodes where clients unintentionally shared individual data. In light of these episodes, the need of apparatuses to offer clients some assistance with controlling access to their common substance is evident. Toward tending to this need, we propose an Adaptive Privacy Policy Prediction (A3P) framework to offer clients some assistance with composing protection settings for their pictures. We look at the part of social connection, picture substance, and metadata as could be expected under the circumstances pointers of clients' security inclinations. We propose a two-level system which as indicated by the client's accessible history on the site, decides the best accessible security approach for the client's pictures being transferred. Our solution relies on an image classification framework for image categories which may be associated with similar policies, and on a policy prediction algorithm to automatically generate a policy for each newly uploaded image, also according to users' social features. 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.

***Keywords*—** A3P, Metadata, Policies, Content sharing, Privacy, Prediction.

I. INTRODUCTION

Pictures are currently one of the key empowering influences of clients' availability. Sharing happens both among beforehand settled gatherings of known individuals or groups of friends (e. g., Google+, Flickr or Picasa), furthermore progressively with individuals outside the clients groups of friends, for purposes of social revelation to offer them some assistance with identifying new companions and find out about associates hobbies and social environment. Be that as it may, semantically rich pictures might uncover content sensitive data [1]. Consider a photograph of an understudies 2012 graduation ceremony, for instance. It could be shared inside of a Google+ circle or Flickr bunch, yet might superfluously uncover the studentsBApos family members and different companions. Sharing pictures inside online substance sharing sites, therefore, may rapidly lead to undesirable exposure and security infringement [3], [4]. Further, the determined way of online media makes it feasible for different clients to gather rich totalled data about the proprietor of the distributed substance and the subjects in the distributed substance [3], [2], [4]. The amassed data can bring about startling introduction of one's social surroundings and lead to mishandle of one's close to home data.

II. EXISTING SYSTEM

1. 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.
2. 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

1. Sharing images within online content sharing sites, therefore, may quickly lead to unwanted disclosure and privacy violations.
2. 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.
3. The aggregated information can result in unexpected exposure of one's social environment and lead to abuse of one's personal information.

III. 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:

1. 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.
2. 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.

ADVANTAGES OF PROPOSED SYSTEM

1. 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.
2. We design the interaction flows between the two building blocks to balance the benefits from meeting personal characteristics and obtaining community advice.

IV. LITERATURE SURVEY

Literature survey is the most important step in software development process. Before improving the tools it is compulsory to decide the economy strength, time factor. Once the programmer's create the structure tools as programmer require a lot of external support, this type of support can be done by senior programmers, from websites or from books.

A. Acquisti and R. Gross , "Imagined communities: Awareness, information sharing, and privacy on the facebook" , pp.36 -58 , 2006

Online social networks such as Friendster, MySpace, or the Facebook have experienced exponential growth in membership in recent years. These networks offer attractive means for interaction and communication, but also raise privacy and security concerns. In this study we survey a representative sample of the members of the Facebook (a social network for colleges and high schools) at a US academic institution, and compare the survey data to information retrieved from the network itself. We look for underlying demographic or behavioural differences between the communities of the network's members and non-members; we analyze the impact of privacy concerns on members' behavior; we compare members' stated attitudes with actual behavior; and we document the changes in behavior subsequent to privacy-related information exposure. We find that an individual's privacy concerns are only a weak predictor of his membership to the network. Also privacy concerned individuals join the network and reveal great amounts of personal information. Some manage their privacy concerns by trusting their ability to control the information they provide and the external access to it. However, we also find evidence of members' misconceptions about the online community's actual size and composition, and about the visibility of members' profiles.

A. Besmer and H. Lipford , "Tagged photos: Concerns, perceptions, and protections" , pp.4585 -4590 , 2009

Online photo sharing applications are increasingly popular, offering users new and innovative ways to share photos with a variety of people. Many social networking sites are also incorporating photo sharing features, allowing users to very easily upload and post photos for their friends and families. For example, Facebook is the largest photo sharing site on the Internet with 14 million photos uploaded daily [2]. Integrating photo sharing within social networking communities has also provided the opportunity for user-tagging, annotating and linking images to the identities of the people in them. This feature further increases the opportunities to share photos among people with established offline relationships and has been largely successful. However, this increased access to an individual's photos has led to these images being used for purposes that were not intended. For example, photos on Facebook profiles have been used by employers [5] and law enforcement [6] to investigate the behavior of individuals. We are focusing on these privacy concerns and needs, as well as exploring ideas for privacy protection mechanisms, for users of social networking sites such as Facebook. In understanding user's current concerns and behaviors, we can design tools they desire, adopt, and ones they will be motivated to use.

M. Bellare, C. Namprempre, and G. Neven Security proofs for identity-based identification and signature schemes. This paper provides either security proofs or attacks for a large number of identity-based identification and signature schemes defined either explicitly or implicitly in existing literature. Here is a framework that helps to explain how the schemes are derived and also permit modular security analyses, which helps to understand, simplify, and unify previous work. We study the generic folklore construction that provides identity-based identification and signature schemes without random oracles.

L. Church, J. Anderson, J. Bonneau and F. Stajano , "Privacy stories: Confidence on privacy behaviors through end user programming" , 2009

In [2] we argued that, in the search to give users meaningful control over their information, we should consider End User Programming techniques as a possible replacement for either

opaque, expert determined choices or the endless proliferation of options that arises from a simplistic application of direct manipulation principles. We describe a work in progress to study the viability of this approach for improving the usability of social network privacy configuration. As suggested in [2] we make use of analytical usability techniques to discuss the usability challenges of the current Facebook interface and to inform the design of our proposed alternative. We then report on a very small (two-user) pilot study and look at challenges that we will address in future design iterations.

V. SYSTEM ARCHITECTURE

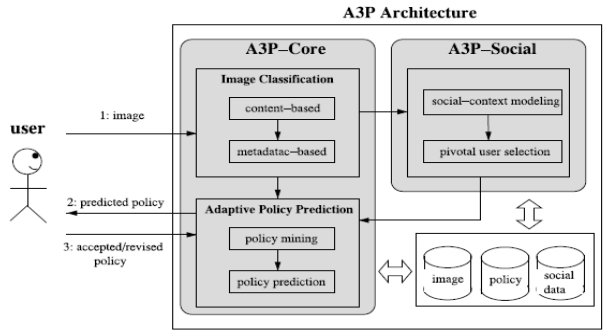

Figure- 1 Architecture

The working of the proposed scheme is very simple, it will provide the classification based on the users preferences. The uploaded images are stored in two categories; first category is to store the images as family and second is store the images as friends. This way security can be provided to the images. Images are also classified based on metadata and image feature classification, i.e. content based image classification.

VI. USE CASE DIAGRAM

The following diagram depicts the use case diagram of the proposed scheme. We need to create user by registering to the application, once it is done, and then request of kind of relationship between the two users is established. Image is uploaded on the social media[1], and based on the security type image can be saved in family circle or friend circle. Image classification takes place, then using the policy prediction, different policies are provided.

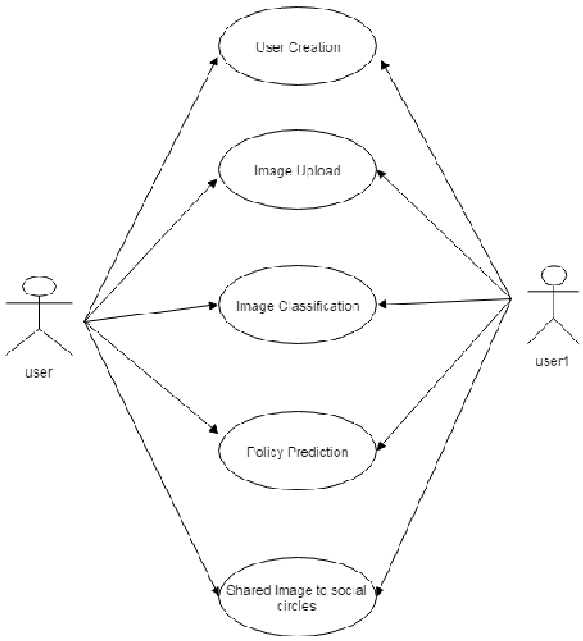

Figure- 2 Data flow diagram of Privacy Policy Inference of User-Uploaded Images on Content Sharing Sites

A3P Framework

Users can provide their policy based on there choice. The system should allow them to choose the best possible solutions for the image security reasons. The algorithm should classify the images based on there metadata or based by there content. Hence making the images more secured.

Our approaches are roused by prominent content sharing destinations (i.e., Facebook, Picasa, Flickr), in spite of the fact that the real usage relies on upon the particular content-administration site structure and execution.

Definition 1. A privacy policy P of user u consists of the following components:

Subject (S): A set of users socially connected to u.

Data (D): A set of data items shared by u.

Action (A): A set of actions granted by u to S on D.

Condition (C): A boolean expression which must be satisfied in order to perform the granted actions.

In the definition, clients in S can be spoken to by their personalities, parts (e.g., family, companion, collaborators), or associations (e.g., non-benefit association, benefit association). D will be the arrangement of pictures in the client's profile. Every picture has a remarkable ID alongside some related metadata such as labels "excursion", "birthday". Pictures can be further assembled into collections. With respect to A, we consider four normal sorts of activities: {view, remark, tag, download}. Last, the condition segment C indicates when the allowed activity is viable. C is a Boolean expression on the grantees' traits like time, area, and age

VII. RESULTS AND DISCUSSION

we investigate the execution of the A3P-Social part by utilizing the first set of information gathering. For every client, we utilize the A3P Social to anticipate strategies and contrast it and a benchmark calculation which does not consider social connections but rather constructs suggestion just with respect to social gatherings that have comparable protection strictness level for same kind of pictures. Utilizing the benchmark approach, we take note of that paying little heed to the individual protection slant of the clients, the best precision is accomplished if there should be an occurrence of unequivocal pictures and pictures ruled by the presence of kids. In both cases, clients keep up more steady arrangements, and our calculation can learn them successfully. The biggest variability, what's more, in this manner more terrible results happen for pictures indicating landscape, where the blunder rate is 15.2 percent. Generally speaking, the exactness accomplished by gathering clients by strictness level is 86.4 percent.

VIII. Conclusion and Future Scope

We have proposed an Adaptive Privacy Policy Prediction (A3P) framework that offers clients some assistance with automating the protection strategy settings for their transferred pictures. The A3P framework gives a thorough structure to induce security inclinations in light of the data accessible for a given client. We additionally adequately handled the issue of icy begin, utilizing social connection data. Our exploratory study demonstrates that our A3P is a viable apparatus that offers huge enhancements over current ways to deal with security.

In future work, we plan to consider same like providing privacy for user uploading image and we can also give the privacy for uploading videos.

IX. REFERENCES

[1] Mr. Pankaj Sareen and Dr. Tripat Deep Singh "Data Security in Cloud", International Journal of Computer Science Engineering (IJCSE) ISSN : 2319-7323, Vol. 4 No.05 Sep 2015

[2]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.

[3] 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.

[4] 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.

[5] M. Ames and M. Naaman, "Why we tag: Motivations for annotation in mobile and online media," in Proc. Conf. Human Factors Comput. Syst., 2007, pp. 971–980.

[6] A. Besmer and H. Lipford, "Tagged photos: Concerns, perceptions, and protections," in Proc. 27th Int. Conf. Extended Abstracts Human Factors Comput. Syst., 2009, pp. 4585–4590.

[7] D. G. Altman and J. M. Bland ,"Multiple significance teJava The complete Reference.

[8] .My SQL Reference Books.

