Middle-East Journal of Scientific Research 24 (Techniques and Algorithms in Emerging Technologies): 553-557, 2016
ISSN 1990-9233;
© IDOSI Publications, 2016
DOI: 10.5829/idosi.mejsr.2016.24.TAET23638

Improve Privacy Policy Inference Model for Network Communication Using Enhanced Parent Policy Control Algorithm

[1]K. Soniya Lakshmi, [2]D. Gowdhami and [2]P. Brindha

[1]Student, Department of CSE, Vivekanandha College of Engineering
for Women, Tamilnadu, India
[2]Assistant Professor, Department of CSE, Vivekanandha
College of Engineering for Women, Tamilnadu, India

Abstract: In recent years, a tremendous growth is seen in online social network. These online social networks offer attractive means for digital social interactions and information sharing, but also raise some security and privacy issues. While online social networks allow users to restrict access to shared data (policy mining), they currently do not provide any mechanism to enforce privacy concerns over data associated with multiple users. Also, it analyzes how the approach can affect the effectiveness of a policy-based collaborative tagging system that supports enhanced web access functionalities, like content filtering and discovery, based on preferences specified by end users.

Key words: Privacy Policy · Social Network · Adaptive Privacy Policy Prediction (A3P) · Filtering

INTRODUCTION

Image sharing within online sites can lead quickly to annoying disclosure and privacy violations. The existence nature of online media makes it possible to collect accumulated information for other users about the owner of the published content and the subjects on it. Result in unexpected exposure to one's social the environment, it leads to abuse one's personal information [1]. A traditional group-based policy management as the proposed baseline and with time improve upon this privacy management model. The human effects are measures with each new enhancement including cluster/user defined relationship group alignment, user privacy sentiment, efficiencies and user perceptions. A user-assisted friend grouping mechanism and it is enhanced a traditional an approach named as group-based policy management. Assisted Friend Grouping leverages prove that the clustering techniques aids the users in grouping their friends in an effective and efficient way.

A new privacy management [2] model is introduced, this is the improved version approach over traditional group-based policy management. The new approach influences on a user's memory and opinion of their friends to set policies for other similar friends named as Same-As Policy Management.

With an example friend, the user associated with the privacy policy by having the forefront of their mind which allows the user to be selective and wary in assigning permissions. Users are thinking of people, not on groups. Visual policy editor takes advantage of friend recognition and minimal the task interruptions; Same - As Policy Management demonstrated improved performance and user perceptions over traditional group-based policy management approaches. Example Friend Selection—two techniques for aiding users to select their example friends that are used in developing policy templates.

Two techniques reduced are the policy authoring times and perceived positively by users. Also to enable the shared data protection associated with multiple users in OSNs a new the proposed. One of the key enablers of users' connectivity is the image.

Related Work: The Proposed works on Privacy setting configuration in social sites, adaptive privacy policy prediction policy system, filtered. Barbara Carminati [4] stated that the existence of online social networks that

Corresponding Author: K. Soniya Lakshmi, Student, Department of CSE,
Vivekanandha College of Engineering for Women, Tamilnadu, India.

include person specific information creates interested opportunities for various applications ranging from marketing to community organization. On the other hand, security and privacy concerns need to be addressed for create such applications. Improving social network access control systems appear as the first step toward addressing the existing security and concerns related to online social networks. To address some of the current limitations, they have created an experimental social network using synthetic data which they then used to test of the semantic reasoning based approaches they have previously suggested.

Yuan Cheng [5] stated that users and resources in online social networks (OSNs) are interconnected via various types of relationships. In particular, user-to-user relationships form the basis of the OSN structure and play a significant role in specifying and enforcing access control. Individual users and the OSN provider should be allowed to specify which access can be granted in terms of existing relationships. The proposed a novel user-to-user relationship-based access control (UURAC) model for OSN systems that utilizes regular expression notation for such policy specification. They developed a path checking algorithm to determine whether the required relationship path between users for a given access request exists and provide proofs of correctness and complexity analysis for the algorithm.

Catherine Dwyer et [6] stated that it is not well understood how privacy concern and trust influence social interactions within social networking sites. An online survey of two popular social networking sites, Facebook, MySpace, compared perceptions of trust and privacy concern, along with the willingness to share information and develop new relationships. Members of both sites reported similar levels of privacy concern. Facebook, members expressed significantly greater trust in both Facebook, its members and were more willing to share identifying information. Even so, MySpace members reported significantly more experience using the site to meet new people. These results suggest that in online interaction, trust is not as necessary in the building of new relationships as it is in the face to face encounters. They also show that in an online site, the existence of the trust and the willingness to share information do not automatically translate into new social interaction. This study demonstrated online relationships can develop in site where perceived trust [7] and privacy safeguards are weak.

Lujan Fang [8] stated that Privacy is an enormous problem in online social networking sites. While sites such as Facebook, allow users fine-grained control over who can see their profiles, it is dificult for average users to specify this kind of detailed policy they proposed a template for the design of a social networking privacy wizard. The intuition for the design comes from the observation that real users conceive their privacy preferences (which friends should be able to see which information) based on an implicit set of rules. Thus, with a limited amount of user input, it is usually possible to build a machine learning model that concisely describes a particular user's preferences and then use this model to configure the user's privacy settings automatically.

Proposed Work: In addition with existing system approaches, the proposed system takes care of parental control based privacy preserving in various settings level also. For example, web content taken may be from more than one languages. So privacy preserving collaborative tagging if applied to content with multiple languages, then it becomes more effective to fruitful to end users. In addition, unlike existing system where the application is not developed for the experimental system, the proposed system develops a web application in which all the above mentioned processes are carried out and so end users make use of it.

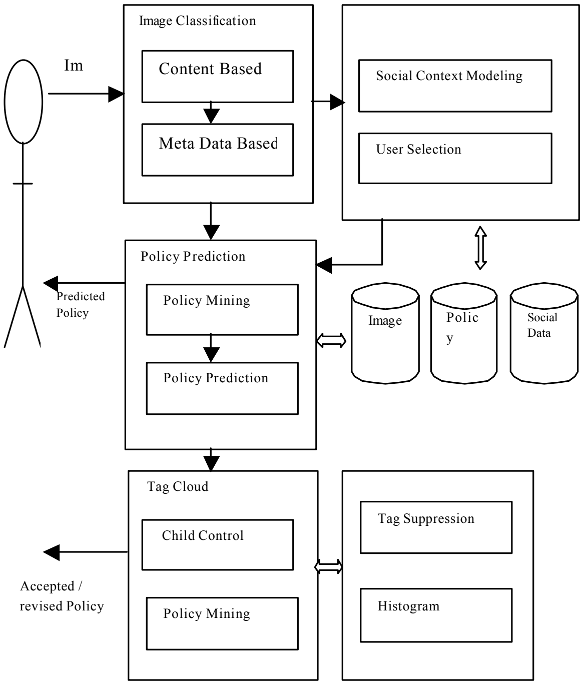
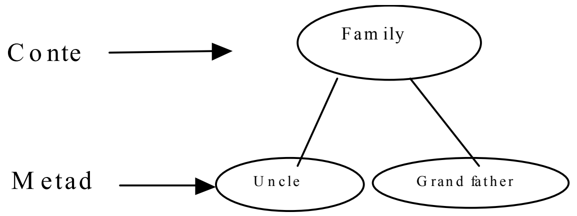


Fig: System Architecture

Content and Metadata Classification: The Proposed method is a content-based classification which is an efficient and accurate image similarity approach. This algorithm compares the defined image signatures based on the quantified and clean version of Haar Wavelet transformation. The wavelet transform in each image encodes frequency and spatial information that are related to image color, size, invariant transform, shape, texture, symmetry, etc. To form signature of an image, a small number of coefficients are selected. Then content similarity among images is determined based on the distance among their image signatures.

$$\mathrm{Dist}_m = w_n.\ D(h_n,h_n^c) + w_{a.}\ D(h_a,h_a^c) + w_v.\ D(h_{v,}h_v^c)$$

Having verified the accuracy of the classifier, we now discuss how it is used in the context of the A3P core. When a user uploads an image, it is handled as an input query image. The signature of the newly uploaded image is compared with the signatures of images in the current image database. To determine the class of the uploaded image, we find its first m closest matches. Later on, if the predicted policy for this new image turns out correct, the image will be inserted into the corresponding image category in our image database, to help refine future policy prediction. In our current prototype, m is set to 25 which is obtained using a small training data set [9].



The metadata-based classification groups [10] images into subcategories under aforementioned 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 from each metadata. The third step is to find a subcategory that an image belongs to the table. Otherwise, a new subcategory will be constructed for this image.

Adaptive Policy Prediction: The policy prediction algorithm provides a predicted of a newly uploaded image to the user. The prediction process consists of three main phase Policy normalization, Policy mining, policy prediction.

Policy normalization by detecting user privacy the sentiment (i.e., an unconcerned user, a pragmatist or a fundamentalist), privacy management models can be automatically tailored specific to the privacy sentiment and needs of the user.

Policy Mining approach for policy mining leverages traditional group-based policy management as our baseline and progressively improve upon this privacy management model. With each new enhancement, we measure their human effects including cluster/user defined relationship group alignment, user privacy sentiment, efficiencies and user perceptions. The thesis introduces a user-assisted friend grouping mechanism that enhances traditional group-based policy management approaches. Assisted Friend Grouping leverages proven clustering [11] techniques to aid users in grouping their friends more effectively and efficiently.

The prediction a new privacy management model that is an improvement over traditional group-based policy management approaches. The new paradigm leverages a user's memory and opinion of their friends to set policies for other similar friends, which we refer to as Same-As Policy Management using a visual policy editor that takes advantage of friend recognition and minimal task interruptions; Same-As Policy Management demonstrated improved performance and user perceptions over traditional the group-based policy management approaches.

Social Context: The social context modeling algorithm that can capture the common social element of users and identify communities formed by the users with similar privacy concerns. We model the ratio of each type of relationship among all contact of a user the social connection.LetR1,…,Rn denote the n-type of relationship among all user. Let N^u_{Ri} denote the number of user connection belonging to relationships type R_i. The connections distribution is represented as below:

$$\mathrm{Conn}:\{N^u_{R1}/\Sigma^n_{i=1}N^u_{Ri},\ldots\ldots\ldots, N^u_{Rn}/\Sigma^n_{i=1}N^u_{Rn}$$

The second step is to identify the group of users who have similar social context and privacy preference. Regarding social context, it rarely happens that users share the same values of all social context attributes.

Several areas to be developed in future, so the application must be upgraded to the new ones required, it is possible to modifications according to new requirements and specifications. The thesis work added the facilities like fast data backup and restoration in case of data loss situations and planned to share the multimedia content data. The policy creation process is improving security [12] in advance automatic configuration for social relationship between users.

RESULTS

The output of secure image retrieval using parent control policy Algorithm in automatic setting privacy preserving. Takes care of parental control based privacy preserving in various settings level also. For example, web content may be from more than one languages. So privacy-preserving collaborative tagging if applied to content with multiple languages, then it becomes more effective to fruitful to the end users. The experimental study proves that the A3P is a practical tool that offers significant improvements over current approaches to privacy.

User Wise Processed: Table 1.1 is describing the experimental result for user wise process result the proposed system. The table contains user id, share id count, comment count details, thread count details and replies details count are shown the below.

Table 1.1: Table Representation For User-wise Processed Result

User Id	Share	Comment	Thread	Replies
1	1	2	1	4
2	1	2	3	1
3	0	1	1	3
4	2	3	2	4
5	4	2	0	5

Fig 1.1 is describing the experimental result for wise user process result in the proposed system.

They are several comment, like, share, post, notification block, poke, privacy and account setting and then the sharing the content and metadata file sharing by using privacy policy or privacy preference.The figure contains user id, share id count, comment count details, thread count details and replies details count shown as below.

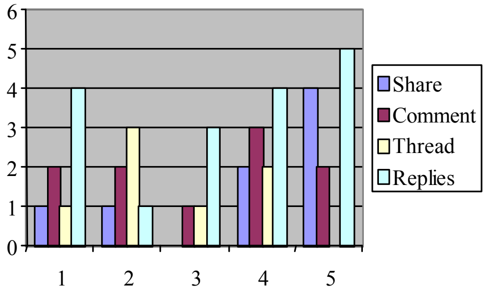


Fig. 5.1: Chart Representations For User-wise Processed Result

Photo Wise Access Details: Table 1.2 is describing the experimental result for photo wise access details in the proposed system. The table contains photo id, view details, comment details and share details count are shown as below

Table No: 1.2: Table Representations for Photo Access Details By User

PHOTO ID	VIEW	COMMENT	SHARE
1	10	15	2
2	15	6	3
3	12	5	2
4	9	5	1
5	6	6	0

Fig 1.2 is describing the experimental result for photo wise access details in proposed system. The figure contains photo id, view details, comment details and share details count are shown below

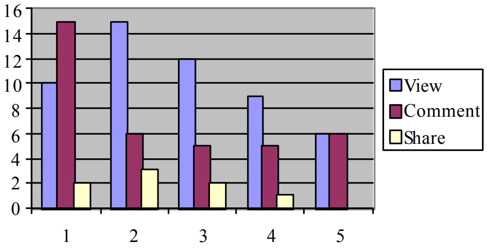


Chart No: 1.2: Chart Representations for Photo Access Details By User

REFERENCES

1. Sriram, B., D. Fuhry, E. Demir, H. Ferhatosmanoglu and M. Demirbas, 2010. Short Text Classification in Twitter to Improve Information Filtering, Proc. 33rd Int'l ACM SIGIR Conf. Research and Development in Information Retrieval (SIGIR '10), pp: 841-842.
2. Strater, K. and H. Richter, 2007. Examining Privacy and Disclosure in a Social Networking Community, Proc. Third Symp. Usable Privacy and Security (SOUPS '07), pp: 157-158, 2007. Rackspace Mosso. http://www.mosso.com/
3. Golbeck, J., 2006. Combining Provenance with Trust in Social Networks for Semantic Web Content Filtering, Proc. Int'l Conf. Provenance and Annotation of Data, L. Moreau and I. Foster, eds., pp: 101-108.
4. Vanetti, M., E. Binaghi, B. Carminati, M. Carullo and E. Ferrari, 2010. Content-Based Filtering in On-Line Social Networks, Proc. ECML/PKDD Workshop Privacy and Security Issues in Data Mining and Machine Learning (PSDML '10), 2010.

5. Cheng, Y., J. Park and R. Sandhu, 2012. A user-to-user relationship-based access control model for online social networks. In Data and applications security and privacy XXVI (pp: 8-24). Springer Berlin Heidelberg.
6. Dwyer, C., S. Hiltz and K. Passerini, 2007. Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace. AMCIS 2007 proceedings, pp: 339.
7. Garfinkel, T., B. Pfaff, J. Chow, M. Rosenblum and D. Boneh, 2003. Terra: a virtual machine-based platform for trusted computing. In ACM Symposium on Operating Systems Principles, pp: 193-206. ACM.
8. Fang, L. and K. LeFevre, 2010. Privacy wizards for social networking sites. In: WWW '10: Proceedings of the 19th international conference onWorld wide web. pp: 351–360. ACM, New York, NY, USA (2010)
9. Lewis, D.D., R.E. Schapire, J.P. Callan and R. Papka, 1996. Training algorithms for linear text classifiers. In Proceedings of the 19th Annual International ACM SIGIR Conference on Research and Development in Information Retrieval (SIGIR 96), pp: 298-306.
10. Koller, D. and M. Sahami, 1997. Hierarchically classifying documents using very few words. In International Conference on Machine Learning (ICML'97), pp: 170-178, Nashville, 1997.
11. Banerjee, S., K. Ramanthan and A. Gupta, 2007. Clustering short text using Wikipedia. In Proc. SIGIR (Amsterdam, The Netherlands, July 2007), pp: 787-788.
12. England, P. and J. Manferdelli, 2006. Virtual machines for enterprise desktop security. Information Se0curity Technical Report, 11(4): 193-202.