Secure Enhanced Privacy Policy in Content Sharing Sites Using Face-To-Face Key Distribution Scheme

Dr.Bhupathi Raju Venkata Rama Raju,
Assistant Professor, Department of Computer Science, Joseph Arts and Science College, Thirunavalur, Villupuram, TamilNadu, India

Abstract-- User Image sharing social site 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 an Adaptive Privacy Policy Prediction (A3P) system to help users compose privacy settings for their images. The 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 user's social features. Image Sharing takes place both among previously established groups of known people or social circles and also increasingly with people outside the users social circles, for purposes of social discovery-to help them identify new peers and learn about peers interests and social surroundings, Sharing images within online content sharing sites, therefore, may quickly lead to unwanted disclosure. The aggregated information can result in unexpected exposure of one's social environment and lead to abuse of one's personal information.

Keywords-- *Adaptive Privacy Policy Prediction (A3P), Content sharing sites (CSS), Quality of Service (QoS)*

I. INTRODUCTION

A. Background of the Study

With the evolution of the Web, various identity management models and privacy technologies have been introduced to solve the identity and privacy issues on the Web. In Web 1.0, most identity management system models such as silo model, centralized model, and federated model are designed from organization's perspective. In this environment, user's privacy concern is focused on how much user's information is stored by service providers and how much user's information is shared with other parties. Moreover, it is difficult for users to obtain information about actual data practices. In other words, privacy concern is raised by storing the user's information in service providers. To reduce this privacy concern, various privacy technologies such as P3P, APPEL and PREP have been introduced. These technologies describe the service provider's privacy policy and user's privacy preference in a machine-readable form, and provide comparison mechanisms to help users to be aware of the service provider's privacy policy practice.

With the introduction of Web 2.0, the digital identity industry recognized that existing identity management models are designed without consideration of user experience, which lead the proposal of the user-centric identity management model that allows users to control their own digital identities in the middle of the transaction between identity providers and service providers. Therefore, users have more rights and control over their identities. The users are able to decide which identity attributes they want to share with other serviceproviders in the middle of transaction. However, the rapid growth of online social networking services in the Web 2.0 changes the user's privacy game. Hundreds of millions of users have accounts on social networking sites. Users build social connections with families, friends, and coworkers by sharing various contents via their profile pages. Updating the user profile pages with attractive content is a form of self-expression that increases the interactions between friends within the social networking sites. The posted content on the user's profile pages is shared with friends or others in public, but the users are often not aware of the size of the viewers accessing the content on their profile. The posted content can be re-distributed by the viewers, and eventually the content can be shared with unintended users who were not explicitly allowed to view that content. Such open sharing availability of social networking sites exposes the users to a number of privacy risks. Therefore, how to control the sharing of content with friends on the social networking sites becomes critical to protect the user's privacy.

B. Data Mining – An Introduction

Generally, data mining (sometimes called data or knowledge discovery) is the process of analyzing data from different perspectives and summarizing it into useful information - information that can be used to increase revenue, cuts costs, or both. Data mining software is one of a number of analytical tools for analyzing data. It allows users to analyze data from many different dimensions or angles, categorize it, and summarize the relationships identified. Technically, data mining is the process of finding correlations or patterns among dozens of fields in large relational databases. In the current era of information explosion, the amount of data generated in numerous research domains, such as business, social media, life science, engineering, and medicine, is rapidly growing; some examples are indicated in Figure 1.1. A study by International Data Corporation (IDC) in 2012 predicted that the digital universe will grow up to 40,000 exabytes, or 40 trillion gigabytes by 2020. The rise of Big Data has led to the development of fast and efficient data mining methods for powerful data analysis tools that explore the tremendous amount of data and turn them into useful knowledge.

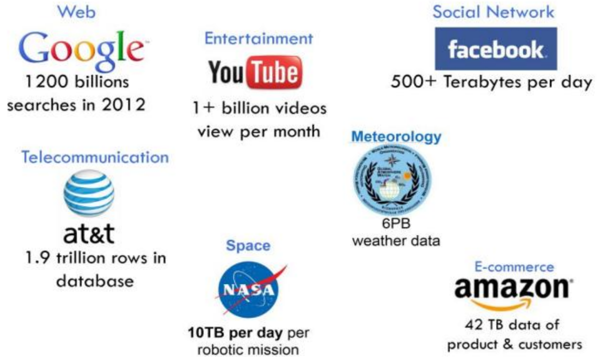
Web
Google
1200 billions searches in 2012
Entertainment
YouTube
1+ billion videos view per month
Social Network
facebook
500+ Terabytes per day
Telecommunication
at&t
1.9 trillion rows in database
Meteorology
6PB weather data
Space
NASA
10TB per day per robotic mission
E-commerce
amazon
42 TB data of product & customers

Figure 1: The growth of world's largest databases

C. Knowledge Discovery in Databases

Knowledge discovery from databases (KDD) is a nontrivial process of identifying valid, novel, potentially useful, and ultimately understandable patterns in data. This process normally consists of multiple steps as shown in Figure 1.2, including data cleaning, data integration, data selection, data mining, evaluation and interpretation:

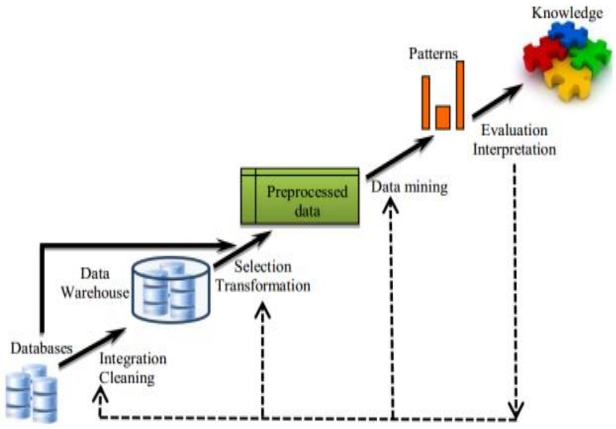

Figure 2: Knowledge discovery in databases

a. Data integration

In many cases, data to be mined are collected and unified from multiple data sources to provide cleansing, consistent and enough essential data for pattern discovery and to enhance the quality of extracted patterns. For large data projects,the integrated data can bestored in a data warehouse. This step can be ignored if the collected data meet certain data integration criteria.

b. Data Cleaning

The original databases may contain noise and inconsistent data which have significant impact on the quality of knowledge to be found by the mining task. This step is done to eliminate noise and errors when possible as well as to handle missing data and other issues of data integration such as mapping the data to a single naming convention.

c. Data selection

A specific data analysis task may require a portion of availabledata instead of the entire data source. This step queries relevant data from the database that will be used as input for the mining step.

d. Data transformation

Data retrieved from database can be converted and consolidated into appropriate forms required by the mining step by operations like formatting, normalization, summarization and/or aggregation. In some cases, data dimensionality reduction methods are also applied to generate invariant representations of the data to reduce the workload and improve the quality of mined patterns. This step is sometimes performed before the data selection.

e. Data mining

This is the central step of the KDD process where intelligent method sare applied to extract data patterns. The selection of the data mining methods and their appropriate parameters is done based on the data mining requirements and data formats.

f. Evaluation and Interpretation

Pattern evaluation identifies the truly interesting patterns representing knowledge. We can utilize the assessment results to modify the computing methods used in each step or loop back to any step of the KDD process untilthe generated patterns reasonably meet the application requirements. The interpretation, in addition, makes the mined patterns easier to understand by human beings by, but not limited to, using some visual forms. For many cases, the patterns are then used as the input of intelligent computing systems.

II. RELATED WORK

Content-based retrieval is ultimately dependent on the features used for the annotation of data and its efficiency is dependent on the invariance and robust properties. The Polar Fourier Transform (PFT) is similar to the Discrete Fourier Transform in two dimensions but uses transform parameters radius and angle rather than the Cartesian co-ordinates. To improve implications for content based retrieval of natural images where there will be a significantly higher number of textures.

Local radial symmetryis to identify regions of interest within a scene. A facial feature detector and as a generic region of interest detector the new transform is seen to offer equal or superior performance to contemporary techniques. The method has been demonstrated on a series of face images and other scenes, and compared against a number of contemporary techniques from the literature. Equal or superior performance on the images tested while offering significant savings in both the computation required and the complexity of the implementation.

The refining process is formulated as an optimization framework based on the consistency between “visual similarity” and “semantic similarity” in social images. An image retagging scheme that aims at improving the quality of the tags associated with social images in terms of content relevance.

Peter F. Klemperer developed a tag based access control of data shared in the social media sites. An approach that produces access-control policies from photo management tags. Every photo is included with an access network for mapping the photo with the participant’s friends. The contributor can choose apposite preference and access the data. Photo tags can be classified as managerial or unrestrained based on the user needs. There are several significant limitations to our study design. First, our outcomes are limited by the participants we conscript and the photos they offered. A second set of limitations apprehension our use of machine generated access-control rules. The algorithm has no admittance to the context and significance of tags and no approaching into the policy the contestant proposed when tagging for access control. As an outcome, some rules become visible strange or random to the contributor, potentially pouring them in the direction of explicit policy-based tags like “private” and “public.

FabeahAdu-Oppong developed the privacy settings depends on the model of social circles. It facilitates a web based explanation to defend personal information. The technique named Social Circles Finder; automatically construct the friend’s list. It is a process that studies the social circle of a person and categorizes the concentration of relationship and as a result social circles offer a meaningful labeling of friends for surroundings privacy policies. The relevance will recognize the social circles of the subject but not show them to the subject. The subject will then be asked questions about their motivation to share a piece of their individual information. Based on the respond the function finds the visual graph of users.

SergejZerr proposes a approach Privacy-Aware Image Classification and Search to robotically detect private images, and to facilitate privacy-oriented image search. It coalesce textual Meta data images with assortment of visual features to facilitate security strategy. In this the chosen image features (edges, faces, color histograms) which can help differentiate between natural and man-made objects/prospect (the EDCV feature) that can indicate the existence or absence of meticulous objects (SIFT). It uses different classification models qualified on a large scale dataset with isolation assignments achieved through a social explanation game.

Anna CinziaSquicciarini developed an Adaptive Privacy Policy Prediction (A3P) system, a free privacy settings system by robotically produces personalized policies. The A3P system levers user uploaded images based on the person's individual characteristics and images content and metadata. The A3P system consists of two components: A3P Core and A3P Social. When a user uploads a data like image, the image will be first sent to the A3P-core. The A3Pcore organizes the image and resolves whether there is a need to appeal to the A3P-social. The disadvantage is mistaken privacy policy production in case of the lack of Meta data information about the images. Also guide creation of Meta data log data information direct to imprecise classification and also contravention privacy. In the past years an incredible growth on Online Social Networks like Facebook, Orkut and Twitter is seen. These OSNs not only propose gorgeous means for virtual social communications and data sharing, but also elevate a number of security issues.

Although OSNs allow a single user to admission to her or his data, they presently do not provide any device to implement privacy protection over data connected with large number of users, departure privacy contravention largely unanswered and leading to the probable confession of information that at least one user proposed to keep private. This paper analyses an assortment of privacy and security issues in OSNs. OSNs come across different types of attacks such a fake identity, Sybil harass, uniqueness clone attacks, The main aim is to augment the privacy and security in OSNs which is one of the Quality of Service (QoS) issues and thus declining the attacks and problems. This paper is a survey which is more detailed to representation the various attacks and privacy models in OSNs with deference to augmentation of security and privacy.

PViz Comprehension Tool, an interface and system that corresponds more directly with how users model groups and privacy policies applied to their networks was developed by Alessandra Mazzia. According to automatically-constructed, natural sub-groupings of friends, and at different levels of granularity PViz allows the user to understand the visibility of her profile. PViz is better than other current policy comprehension tools Facebook's Audience View and Custom Settings page. It also addresses the important sub-problem of producing effective group labels since the user must be able to identify and distinguish automatically-constructed groups.

Privacy Suites is proposed by Jonathan Anderson which allows users to easily choose ―suites" of privacy settings. Using privacy programming a privacy suite can be created by an expert. Privacy Suites could also be created directly through existing configuration UIs or exporting them to the abstract format. To the members of the social sites the privacy suite is distributed through existing distribution channels. Transparency is the main goal, which is essential for convincing influential users that it is safe to use. The disadvantage of a rich programming language is less understandability for end users. To verify a Privacy Suite sufficiently high-level language and good coding practice, motivated users are able.

Privacy-Aware Image Classification and Search is a technique to automatically detect private images, and to enable privacy-oriented image search introduced by SergejZerr. To provide security policies technique combines textual Meta data images with variety of visual features. It uses various classification models trained on a large scale dataset with privacy assignments obtained through a social annotation game. In this the selected image features (edges, faces, color histograms) which can help discriminate between natural and man-made objects/scenes (the EDCV feature) that can indicate the presence or absence of particular objects (SIFT).

A tag based access control of data is developed by Peter F. Klemperer. It is a system that creates access-control policies from photo management tags. Every photo is incorporated with an access grid for mapping the photo with the participant's friends. A suitable preference can be selected by participants and access the information. Based on the user needs photo tags can be categorized as organizational or communicative. There are several important limitations .First, our results are limited by the participants recruited and the photos provided by them. Machine generated access-control rules are the second limitation. Algorithm used here has no access to the context and meaning of tags and no insight into the policy the participant intended when tagging for access control. Hence, some rules appeared strange to the participants who makes them to tag explicitly like ―private and public.

YourPrivacyProtector is a recommender system proposed by KambizGhazinour that understands the social internet behavior of their privacy settings and recommending reasonable privacy options. The parameters used are user's personal profile, User's interests and User's privacy settings on photo albums.With the help of these parameters the system constructs the personal profile of the user. For a given profile of users it will automatically learn and assign the privacy options. It detects the possible privacy risks and allows users to see their current privacy settings on their social network profile, namely Facebook, and monitors frequently. Necessary privacy settings are adopted based on these risks.

A decentralized authentication protocol, is an access control system proposed by Ching-man Au Yeung based on a descriptive tags and linked data of social networks in the Semantic websites. Here users can specify access control rules based on open linked data provided by other parties and it allows users to create expressive policies for their photos stored in one or more photo sharing.

Adaptive Privacy Policy Prediction (A3P) system is introduced by Anna CinziaSquicciarini. Personalized policies can be automatically generated by this system. It makes use of the uploaded images by users and a hierarchical image classification is done. Images content and metadata is handled by the A3P system. It consists of two components: A3P Core and A3P Social. The image will be first sent to the A3P-core, when the user uploads the image. The A3P-core classifies the image and determines whether there is a need to invoke the A3P-social.When Meta data information is unavailable it is difficult to generate accurate privacy policy. This is the disadvantage of this system. Privacy violation as well as inaccurate classification will be the after effect of manual creation of Meta data log information.

Ching-man Au Yeung et al proposed an access control system based on a decentralized authentication protocol, descriptive tags and linked data of social networks in the Semantic Web. It allows users to create expressive policies for their photos stored in one or more photo sharing sites, and users can specify access control rules based on open linked data provided by other parties.

Danezisetalproposed a machine-learning based approach to automatically extract privacy settings from the social context within which the data is produced. It develops privacy settings based on a concept of “Social Circles” which consist of clusters of friends. User’s privacy preferences for location-based data based on location and time of day.

FabeahAdu-Oppong et al developed concept of social circles. It provides a web based solution to protect personal information. The technique named Social Circles Finder, which automatically generates the friend’s list. It is a technique that analyses the social circle of a person and identifies the intensity of relationship and therefore social circles obtained a meaningful categorization of friends for setting privacy policies. The application will identify the social circles of the subject but not show them to the subject. The subject will then be asked questions about their willingness to share a piece of their personal information. Based on the answers the application finds the visual graph of users.

Fang et al proposed a privacy wizard to assist users grant privileges to their friends. The wizard asks users to first assign privacy labels to selected friends, and then uses this as input to construct a classifier which divides friends based on their profiles and automatically assign privacy labels to the unlabeled friends.

III. PROBLEM STUDY

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. As far as images, authors in have presented an expressive language for images uploaded in social sites. This work is complementary to ours as we do not deal with policy expressiveness, but rely on common forms policy specification for our predictive algorithm. In addition, there is a large body of work on image content analysis, for classification and interpretation, retrieval, and photo ranking, also in the context of online photo sharing sites. Of these works, probably the closest to ours explores privacy-aware image classification using a mixed set of features, both content and meta-data. This is however a binary classification (private versus public), so the classification task is very different than ours. Also, the authors do not deal with the issue of cold-start problem.

Content sharing sites (CSS) such as Google+, Picasa, Facebook, and Twitter have become one of the fastest emerging e-services. There are numerous issues affected these e-services like security and privacy. They where many advance projected for the privacy preserving policy for this social network. Some advance may cause problem since of unproductive algorithms. Many approaches were executed which failed to avoid the data exploitation and privacy problem. Most of the trouble we had studied in the existing system was acknowledged in terms of privacy and security of image data through the communication from one to an additional user in social network. Privacy threat is one of the dangerous issues in these social networks. Since it is emerging service and consistent to communicate, it is also a new harass ground for data hackers, they can easily exploitation the data.

IV. PROPOSED DESIGN

In this section, we are implementing an Adaptive Privacy Policy Prediction (A3P) system which will provide users a hassle free privacy settings experience by automatically generating personalized policies.The A3P framework is discussed as below: Privacy Policies are privacy preferences expressed by the user about their content disclosure preferences with their socially connected users.We define the privacy policies as follows:

Definition: A Privacy policy P can be described foruser U by:

1. Subject(S): A Set of users socially connected to user U.
2. Data (D): A set of data items shared by U.
3. Action (A): A set of actions granted by U to S on D.
4. Condition (C): A Boolean expression which must be satisfied in order to perform the granted actions.

In the above definition, Subject(S) can be user's identities, relations such as family, friend, coworkers, etc. and organizations. Data(D) consists of all the images in the user's profile. Action(A) considers four factors: View, Comment, tags and Download. Lastly the Condition(C) specifies whether the actions are effective or not. Example 1. Joe wants to allow her friends and family to view and comment on images in the album named “birthday_album” and the image named “cake.jpg” before year 2015.The policy for her privacy preference will be P: [{friend, family}, {birthday_album, cake.jpg},{view ,comment}, (date< 2015)] allowed.

A. Architecture of A3P

A3P stands for Adaptive Privacy Policy Prediction system which helps users to derive the privacy settings for their images. The A3P Architecture consists of followings blocks: A3P Core.

1. Metadata based Image classification.
2. Adaptive policy prediction.
3. Look-Up Privacy Policies
4. Database

A3P Core classifies the images with the help of the Metadata and also predicts the policies depending upon the behavior of the user. The Look-up Privacy Policy looks if the image or similar type of image already exists which can be given with similar privacy policies. If similar type of image doesn’t exist then it looks for all the policies and lets user choose the policies.

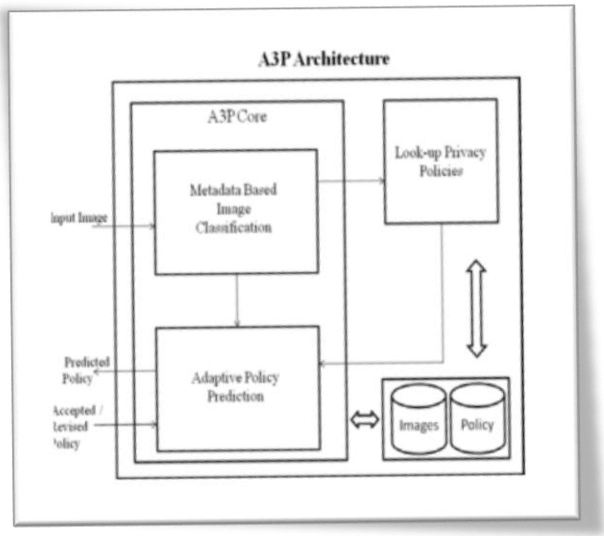

Figure 3: System Architecture of A3P system

B. Working Of A3P Core:

The A3P Core consists of two major blocks of the framework.

1. Metadata based Image Classification
2. Adaptive Policy Prediction

Every image of the user gets classified based on the metadata and then its privacy policies are generalized. With the help of this approach, the policy recommendation becomes easy and more accurate. Based on the Classification based on metadata the policies are applied to the right class of images. Moreover combining the image and classification and policy prediction would enhance the system's dependency.

***a. Metadata based image classification*:**

As mentioned, the metadata based Image classification groups the images into sub-categories with the help of following three steps.
Step 1: This process obtains the keywords from the metadata of the image. Tags, Comments and Captions are included in our metadata through which the keywords are obtained. After obtaining the keywords our task is to identify all nouns, verbs and adjectives and store them into a metadata vector such as

Tnoun= {t1, t2, t3… tk},
Tverb={t1, t2, t3… tj},
Tadjective= {t1, t2, t3... tl} where k,j and l are thetotal number of nouns, verbs and adjectives respectively.

Step 2: This process is to attain a typical hypernym from each metadata vector. The hypernym is denotedby h and first retrieved for every ti. This hypernym can be represented as h={(v1,f1), (v2,f2),….}.Here v denotes as the hypernym and f denotes its frequency. For example, consider a metadata vector T={, "Job", "Promotion","Party"}.With the help of this set we can say that Job and Promotion have the same hypernym work whereas Party has a hypernym Activity. Hence, we can show the hypernym list as h= {(work, 2), (Activity, 1)}.From this list we select the hypernym with the highest frequency.
Step 3:This process is to obtain the subcategory in which the image fits in. This step is an incremental procedure in which the first image forms a subcategory and the hypernyms of the image are also allotted to their respective subcategory. For every new incoming image, the distance between these hypernyms and each category is computed and the closest subcategory for that image is discovered.

b. Adaptive Policy Prediction

This part deals with the privacy concerns of the user by deriving the privacy policies for the images. The Adaptive Policy Prediction consists of two following sub-parts:

1. Policy Mining
2. Policy Prediction

Policy mining deals with data mining of policies for similar categorized images and Policy prediction applies prediction algorithm to predict the policies.

a. Policy mining

The privacy policies are the privacy preferences expressed by the users. Policy mining deals with mining of these policies by applying different association rules and steps. It follows the order in which a user defines a policy and decides what rights must be given to the images. This hierarchical mining approach starts by looking the popular subjects and their popular actions in the policies and finally for conditions. It can be thoroughly reviewed with the help of following steps.

Step 1: This process apply association rule mining on the subject components of the policies of the new image. With the association rule mining we select the best rules according to one of the interestingness measure i.e., support and confidence which gives the most popular subjects in policies.

Step 2: This process apply association rule mining on the action components. Similar to the first step we will select the best rules which will give most popular combinations of action in policies. Step 3: This process mine the condition component in each policy set. The best rules are selected which gives us a set of attributes which often appear in policies.

b. Policy Prediction

The policy mining phase may give us many policies but our system needs to show the best one to the user. Thus, this approach is used to choose the best policy for the user by obtaining the strictness level. The Strictness level decides how "strict" a policy is by returning an integer value. This value should be minimum to attain high strictness. The strictness can be discovered by two metrics: major level and coverage rate. The major level is determined with the help of combinations of subject and action in a policy and coverage rate is determined using the condition statement. Different integer values are assigned according to the strictness to the combinations and if the data has multiple combinations we will select the lowest one. Coverage rate provides a fine-grained strictness level which adjusts the obtained major level. For example a user has to 5 friends and two of them are females. Hence if he specifies policy as "friends"=male, then the coverage rate can be calculated as (3/5)=0.6. Hence, the image is less restricted if the coverage rate value is high.

CONCLUSION

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.

Sharing images within online content sharing sites,therefore,may quickly leadto 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.

References

[1] R. Datta, D. Joshi, J. Li, and J. Wang, "Image retrieval: Ideas, influences, and trends of the new age" IEEE Transaction on Cloud Computing, Vol. 2, NO. 4, OCTOBER-DECEMBER 2014.

[2] P.R. Hill, C.N. Canagarajah and D.R. Bull, "Rotationally Invariant Texture Based Features" IEEE Computer Society 1089- 7801/15/$31.00 c 2015 IEEE.

[3] Kaitai Liang, Joseph K. Liu, Rongxing Lu, Duncan S. Wong, "Privacy Concerns for Photo Sharing in Online Social Networks" IEEE Computer Society 1089-7801/15/$31.00 c 2015 IEEE.

[4] P. Klemperer, Y. Liang, M. Mazurek, M. Sleeper, "Tag, you can see it!: Using tags for access control in photo sharing" IEEE Transaction on Engineering Management, Vol. 62, NO. 3, AUGUST 2015.

[5] D. Liu, X.-S. Hua, M. Wang, and H.-J.Zhang, “Retagging social images based on visual and semantic consistency” IEEE Transaction on Image Processing, VOL. 24, NO. 11, NOVEMBER 2014.

[6] G. Loy and A. Zelinsky, “Fast radial symmetry for detecting points of interest” IEEE Transaction on Pattern Analysis and Machine Intelligence, Vol. 25, NO.8, AUGUST 2014.

[7] LinkeGuo, Chi Zhang, and Yuguang Fang, “A Trust-Based Privacy-Preserving Friend Recommendation Scheme for Online Social Networks” IEEE Transaction on Dependable and Secure Computing, Vol. 12, NO. 4, JULY/AUGUST 2015.

[8] XuemingQian, Xian-Sheng Hua, Yuan Yan Tang, and Tao Mei “Social Image Tagging With Diverse Semantics” IEEE Transaction on Cybernetics, Vol. 44, NO. 12, DECEMBER 2014.

[9] S. Zerr, S. Siersdorfer, J. Hare, and E. Demidova, “Privacy-aware image classification and search” IEEE Transaction on Pattern Analysis and Machine Intelligence, Vol. 25, NO. 8, AUGUST 2014.

[10] J. Zhuang and S. C. H. Hoi, “Nonparametric kernel ranking approach for social image retrieval” IEEE Transaction on Knowledge and Data Engineering, Vol. 26, NO. 1, JANUARY 2014.

[11] R. Reichle et al., "A Comprehensive Context Modeling Framework for Pervasive Computing Systems", In Proceedings of the 8th IFIP International Conference on Distributed Applications and Interoperable Systems (DAIS), Oslo, Norway, Springer Verlag, June 2008.

[12] A. Devlic, "Extending CPL with context ontology", In Mobile Human Computer Interaction (Mobile HCI 2006) Conference Workshop on Innovative Mobile Applications of Context (IMAC), Espoo/Helsinki, Finland, September 2006.

[13] W. Dargie, "The Role of Probabilistic Schemes in MultisensorContextAwareness", In Proceedings of the Fifth Annual IEEE International Conference on Pervasive Computing and Communications Workshops (PerComW’07), pp.27-32, March 2007.

[14] S. Wasserman and K. Faust, "Social Network Analysis, Methods and Applications". Cambridge, UK: Cambridge University Press. 1994.

[15] G. Kossinets and D. J. Watts. "Empirical Analysis of an Evolving Social Network", Science 311, pp. 88-90. 2006.

[16] H. Ebel, L-I.Mielsch, and S. Bornholdt. "Scale-free topology of e-mail networks", Phys Rev E 66: 35103. 2002.

[17] W. Aiello, F. Chung, and L. Lu, "A random graph model for massive graphs", Annual ACM Symposium on Theory of Computing, Proceedings of the thirty-second annual ACM symposium on Theory of computing, pp. 171–180, 2000.

[18] J. M. Kleinberg, "Challenges in mining social network data: processes, privacy, and paradoxes". In Proceedings of the 13th ACM SIGKDD international conference on Knowledge discovery and data mining (KDD ’07), pp. 4-5. 2007.

[19] A. Toninelli, R. Montanari, L. Kagal, and O. Lassila. Proteus, "A Semantic Context-Aware Adaptive Policy Model", Eighth IEEE International Workshop on Policies for Distributed Systems and Networks (POLICY '07). IEEE Computer Society, pp. 129-140, 2007.

[20] T. Moses (ed.), "OASIS eXtensible Access Control Markup Language (XACML) Version 2.0". OASIS Standard, 1 Feb 2005.

[21] C. Kamienski, J. Fidalgo, R. Dantas, D. Sadok, and B. Ohlman, "XACML-Based Composition Policies for Ambient Networks", Eighth IEEE International Workshop on Policies for Distributed Systems and Networks (POLICY '07). IEEE Computer Society, pp. 77-86, 2007.

[22] R. Yavatkar, D. Pendarakis, and R. Guerin, "A Framework for Policybased Admission Control", IETF RFC 2753, January 2000.

[23] K. Verlaenen, B. De Win, and W. Joosen, "Policy Analysis Using a Hybrid Semantic Reasoning Engine", Eighth IEEE International Workshop on Policies for Distributed Systems and Networks (POLICY '07). IEEE Computer Society, pp. 193-200, 2007.

[24] The Friend of a Friend (FOAF) project, http://www.foaf-project.org/, last visited on January 2009.

[25] XHTML Friends Network (XFN), http://gmpg.org/xfn/, last visited on January 2009.