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 4, April 2016

Secured Content Sharing Through Social Sites

Halamma T.B, Lavanya .S

M.Tech Student, Dept. of Computer Science and Engineering, The Oxford College of Engineering, Bangalore, Karnataka, India

Assistant Professor, Dept. of Computer Science and Engineering, The Oxford college of Engineering, Bangalore, Karnataka, India

ABSTRACT: With the expanding volume of pictures clients offer through social locales, keeping up security has turned into a noteworthy issue, as showed by a late rush of exposed occurrences where clients unintentionally shared individual data. In light of these episodes, the need of instruments to help clients control access to their mutual substance is obvious. Toward tending to this need, we propose an Adaptive Privacy Policy Prediction [A3P] framework to help clients create security settings for their pictures. We look at the part of social setting, picture substance, and metadata as could be allowed markers 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 arrangement for the client's pictures being transferred. Our answer depends on a picture order system for picture classes which might be connected with comparable approaches, and on an arrangement forecast calculation to naturally produce a strategy for each recently transferred picture, additionally as indicated by clients' social components. After some time, the produced arrangements will take after the advancement of clients' protection state of mind. We give the aftereffects of our broad assessment more than 5,000 approaches, which show the viability of our framework, with forecast correctness's more than 90 percent.

KEYWORDS: Data Services, Content Sharing Services, Social Sites, Policy Prediction, A3P, Forecasting.

I. INTRODUCTION

Images are now one of the key enablers of users' connectivity. Sharing takes place both among previously established groups of known people or social circles (e.g., Google+, Flickr or Picasa), 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. However, semantically rich images may reveal content sensitive information. Consider a photo of a student's 2012 graduation ceremony, for example. It could be shared within a Google+ circle or Flickr group, but may unnecessarily expose the students BApos family members and other friends.

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

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 4, April 2016

II. PROPOSED FRAMEWORK CONTRIBUTIONS

In this framework, we propose an Adaptive Privacy Policy Prediction (A3P) framework which plans to give clients a bother free protection settings experience via consequently producing customized strategies. The A3P framework handles client transferred pictures, and calculates the accompanying criteria that impact one's protection settings of pictures:

- The effect of social environment and individual qualities. Social connection of clients, for example, their profile data and associations with others may give helpful data in regards to clients' security inclinations. For instance, clients keen on photography may get a kick out of the chance to impart their photographs to other novice picture takers. Clients who have a few relatives among their social contacts may impart to them pictures identified with family occasions. Notwithstanding, utilizing regular strategies over all clients or crosswise over clients with comparative attributes might be excessively shortsighted and not fulfill singular inclinations.

- Clients may have definitely distinctive suppositions even on the same sort of pictures. For instance, a security unfavorable individual might will to share all his own pictures while a more moderate individual may simply need to impart individual pictures to his relatives. In light of these contemplations, it is imperative to discover the adjusting point between the effect of social environment and clients' individual attributes so as to foresee the strategies that match every individual's needs.

- In addition, people may change their general state of mind toward security over the long haul. Keeping in mind the end goal to build up a customized arrangement proposal framework, such changes on protection conclusions ought to be precisely considered.

- The part of picture's substance and metadata. As a rule, comparable pictures regularly bring about comparable protection inclinations, particularly when individuals show up in the pictures. For instance, one may transfer a few photographs of his children and determine that exclusive his relatives are permitted to see these photographs. He may transfer some different photographs of scenes which he took as an interest and for these photographs, he may set protection inclination permitting anybody to view and remark the photographs. Dissecting the visual substance may not be adequate to catch clients' protection inclinations. Labels and other metadata are characteristic of the social connection of the picture, including where it was taken and why, furthermore give a manufactured depiction of pictures, supplementing the data acquired from visual substance investigation.

Comparing to the previously stated two criteria, the proposed A3P framework is involved two primary building hinders (as appeared in Fig. 1): A3P-Social and A3P-Core. The A3P-center spotlights on examining every individual client's own particular pictures and metadata, while the A3P-Social offers a group point of view of protection setting proposals for a client's potential security change. We plan the cooperation streams between the two building pieces to adjust the advantages from meeting individual attributes and getting group exhortation. To survey the pragmatic estimation of our methodology, we fabricated a framework model and performed a broad exploratory assessment. We gathered and tried more than 5,500 genuine approaches created by more than 160 clients.

Our exploratory results exhibit both proficiency and high forecast exactness of our framework. A preparatory discourse of the A3P-center was displayed. In this work, we display an updated form of A3P, which incorporates a broadened arrangement expectation calculation in A3P-center (that is currently parameterized taking into account client bunches furthermore considers conceivable exceptions), and another A3P-social module that builds up the idea of social connection to refine and amplify the forecast force of our framework. We likewise lead extra tries different things with information set gathering more than 1,400 pictures and comparing approaches, and we augment our investigation of the experimental results to reveal more experiences of our framework's execution.

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 4, April 2016

System Design:

The A3P framework comprises of two principle segments: A3P-center and A3P-social. The general information stream is the accompanying. At the point when a client transfers a picture, the picture will be first sent to the A3P-center. The A3P-center arranges the picture and figures out if there is a need to summon the A3P-social.In most cases, the A3P-center predicts strategies for the clients specifically taking into account their chronicled conduct. In the event that one of the accompanying two cases is checked valid, A3P-center will conjure A3P social:

(a) The client does not have enough information for the sort of the transferred picture to direct strategy forecast;
(b) The A3P-center distinguishes the late significant changes among the client's group about their protection rehearses alongside client's increment of person to person communication exercises (expansion of new companions, new posts on one's profile and so forth).

In above cases, it is helpful to answer to the client the most recent security routine of social groups that have comparative foundation as the client. The A3P-social gatherings clients into social groups with comparable social setting and protection inclinations, and constantly screens the social gatherings. At the point when the A3P-social is summoned, it consequently recognizes the social gathering for the client and sends back the data about the gathering to the A3P-center for approach forecast. Toward the end, the anticipated strategy will be shown to the client. On the off chance that the client is completely fulfilled by the anticipated strategy, he or she can simply acknowledge it. Something else, the client can reconsider the arrangement. The real strategy will be put away in the approach vault of the framework for the arrangement forecast of future transfers.

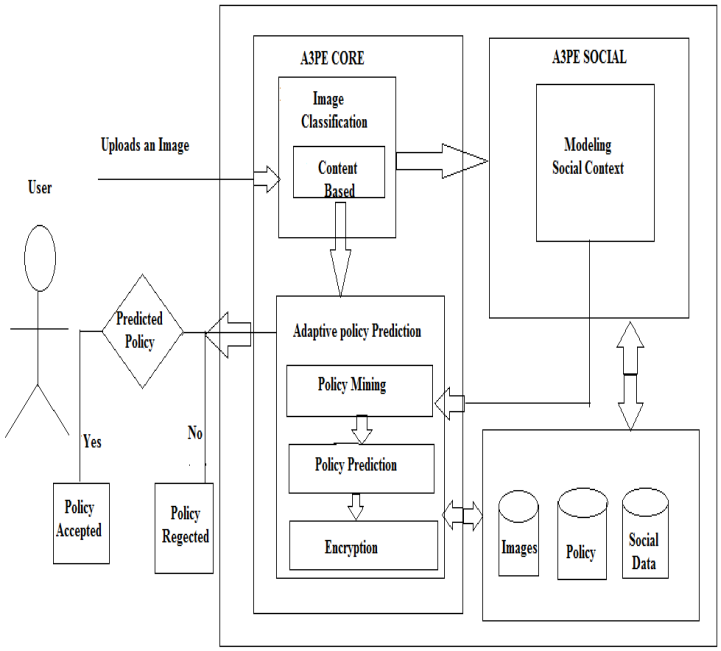

Fig. 1 System Design

III. SECURITY SETTING CONFIGURATION

A few late works have concentrated how to computerize the undertaking of protection settings. Bonneau et al. proposed the idea of protection suites which prescribe to clients a suite of security settings that "master" clients or other trusted

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 4, April 2016

companions have effectively set, so that typical clients can either straightforwardly pick a setting or just need to do minor alteration. Essentially, Danezis proposed a machine-learning based way to deal with naturally separate protection settings from the social connection inside which the information is created.
Parallel to the work of Danezis, Adu-Oppong et al. create security settings in view of an idea of "Groups of friends" which comprise of bunches of companions shaped by apportioning clients' companion records. Ravichandran et al. concentrated how to anticipate a client's security inclinations for area based information (i.e., share her area or not) in view of area and time of day. Tooth et al. proposed a protection wizard to help clients stipend benefits to their companions. The wizard asks clients to first appoint security marks to chose companions, and afterward utilizes this as contribution to develop a classifier which arranges companions in view of their profiles and naturally allocate protection names to the unlabeled companions. All the more as of late, Klemperer et al. concentrated on whether the watchwords and inscriptions with which clients tag their photographs can be utilized to help clients all the more naturally make and keep up access-control strategies.

Their discoveries are in-line with our methodology: labels made for hierarchical purposes can be repurposed to make sensibly exact access-control rules. The previously stated methodologies concentrate on inferring arrangement settings for just qualities, so they for the most part consider social connection, for example, one's companion list. While fascinating, they may not be adequate to address challenges brought by picture documents for which protection may shift considerably due to social connection as well as because of the real picture content. To the extent pictures, creators have introduced an expressive dialect for pictures transferred in social destinations. This work is reciprocal to our own as we don't manage strategy expressiveness; however depend on normal structures approach particular for our prescient calculation.

Likewise, there is a substantial assortment of work on picture content examination, for order and translation, recovery, and photograph positioning, additionally with regards to online photograph sharing locales, for example, Flickr. Of these works, Zerr's work is presumably the nearest to our own. Zerr investigates security mindful picture arrangement utilizing a blended arrangement of components, both substance and meta-information. This is however a double arrangement (private versus open), so the order assignment is altogether different than our own. Likewise, the creators don't manage the issue of icy begin issue.

IV. SUGGESTION SYSTEMS

Our work is identified with some current proposal frameworks which utilize machine learning procedures. Chen et al. proposed a framework named SheepDog to naturally embed photographs into proper gatherings and suggest appropriate labels for clients on Flickr. They receive idea identification to foresee pertinent ideas (labels) of a photograph. Choudhury et al. proposed a suggestion system to interface picture content with groups in online social networking. They portray pictures through three sorts of components: visual elements, client created content labels, and social association, from which they prescribe the no doubt bunches for a given picture.
Additionally, Yu et al. proposed a computerized proposal framework for a client's pictures to recommend reasonable photograph sharing gatherings. There is likewise a vast assemblage of work on the customization and personalization of label based data recovery, which uses strategies, for example, affiliation standard mining. For instance, proposes a fascinating exploratory assessment of a few shared separating calculations to suggest bunches for Flickr clients. These methodologies have an entirely unexpected objective to our methodology as they concentrate on sharing as opposed to securing the substance.

V. A3P INFRASTRUCTURE

Clients can express their protection inclinations about their substance revelation inclinations with their socially associated clients by means of security strategies. We characterize security approaches as per Definition 1. Our arrangements are propelled by well known substance sharing destinations (i.e., Facebook, Picasa, Flickr), despite the fact that the real usage relies on upon the particular substance administration site structure and execution.

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 4, April 2016

Definition-:

A protection strategy P of client u comprises of the accompanying parts:

Subject (S): An arrangement of clients socially associated with u.
Data (D): An arrangement of information things shared by u.
Action (An): An arrangement of activities allowed by u to S on D.
Condition (C): A boolean expression which must be fulfilled with a specific end goal to perform the conceded activities.

In the definition, clients in S can be spoken to by their characters, 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 special ID alongside some related metadata like labels "excursion", "birthday". Pictures can be further assembled into collections.

With respect to A, we consider four basic sorts of activities: {view, remark, tag, download}. Last, the condition segment C indicates when the allowed activity is powerful. C is a Boolean expression on the grantees' traits like time, area, and age. For better understanding, an illustration strategy is given beneath.

Illustration-1: Alice might want to permit her companions and collaborators to remark and label pictures in the collection named "excursion collection" and the picture named "summer.jpg" before year 2012. Her security inclinations can be communicated by the accompanying approach:

P: {friend, coworker}, {vacation album, summer.jpg}, {comment, tag}, (date< 2012).

There are two noteworthy segments in A3P-center: (an) Image arrangement and (b) Adaptive approach forecast.

For every client, his/her pictures are initially characterized in light of substance and metadata. At that point, protection strategies of every classification of pictures are broke down for the approach forecast. Embracing a two-phase methodology is more appropriate for strategy suggestion than applying the normal one-phase information mining ways to deal with mine both picture elements and arrangements together. Review that when a client transfers another picture, the client is sitting tight for a suggested arrangement. The two-phase approach permits the framework to utilize the primary stage to group the new picture and discover the competitor sets of pictures for the consequent arrangement proposal.

With respect to the one-phase mining approach, it would not have the capacity to find the right class of the new picture since its characterization criteria needs both picture components and arrangements while the strategies of the new picture are not accessible yet. In addition, joining both picture elements and strategies into a solitary classifier would prompt a framework which is exceptionally needy to the particular sentence structure of the strategy. On the off chance that an adjustment in the bolstered approaches was to be presented, the entire learning model would need to change.

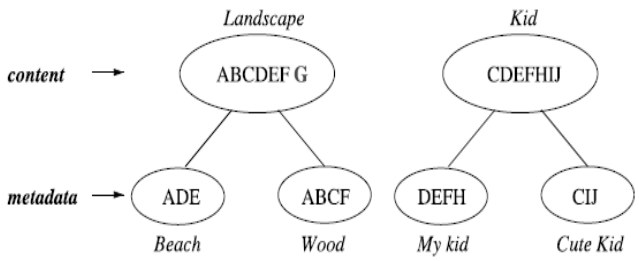

Fig. 2 Picture Classification – 2 Levels

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 4, April 2016

VI. PICTURE CLASSIFICATION

To get gatherings of pictures that might be connected with comparable protection inclinations, we propose a various leveled picture grouping which characterizes pictures initially taking into account their substance and afterward refine every classification into subcategories in view of their metadata. Pictures that don't have metadata will be gathered just by substance. Such a various leveled grouping gives a higher need to picture content and minimizes the impact of missing labels. Note that it is conceivable that some pictures are incorporated into various classes the length of they contain the run of the mill content components or metadata of those classifications. Also, Fig. 2 demonstrates a case of picture grouping for 10 pictures named as A, B, C, D, E, F, G, H, I, J, individually. The substance based grouping makes two classes: "scene" and "child". Pictures C, D, E and F are incorporated into both classifications as they show kids playing outside which fulfill the two topics: "scene" and "child". These two classifications are further isolated into subcategories in view of labels connected with the pictures. Thus, we get two subcategories under every subject individually.
Notice that picture G is not appeared in any subcategory as it doesn't have any label; picture appears in both subcategories on the grounds that it has labels showing both "shoreline" and "wood".

VII. CONTENT-BASED CLASSIFICATION

Our way to deal with substance construct arrangement is situated in light of an effective but exact picture similitude approach. In particular, our order calculation thinks about picture marks characterized in view of evaluated and purified variant of Haar wavelet change. For every picture, the wavelet change encodes recurrence and spatial data identified with picture shading, size, invariant change, shape, composition, symmetry, and so forth. At that point, a little number of coefficients is chosen to frame the mark of the picture. The substance similitude among pictures is then dictated by the separation among their picture marks. Our chose likeness criteria incorporate composition, symmetry, shape (outspread symmetry and stage congruency), and SIFT. We additionally represent shading and size. We set the framework to begin from five bland picture classes: (an) unequivocal (e.g., nakedness, savagery, drinking and so on), (b) grown-ups, (c) kids, (d) landscape (e.g., shoreline, mountains), (e) creatures.

As a preprocessing step, we populate the five pattern classes by physically doling out to every class various pictures crept from Google pictures, bringing about around 1,000 pictures for every class. Having substantial picture information set heretofore diminishes the shot of misclassification. At that point, we produce marks of all the pictures and store them in the database. After modifying the settings of our substance classifier, we led some preparatory test to assess its exactness.

Decisively, we tried our classifier it against a ground-truth information set, Image-net.org. In Image-net, more than 10 million pictures are gathered and grouped by wordnet structure. For every picture class, we utilize the principal half arrangement of pictures as the preparation information set and order the following 800 pictures. The arrangement result was recorded as right if the synset's primary pursuit term or the immediate hypernym is returned as a class. The normal exactness of our classifier is above 94 percent. Having checked the exactness of the classifier, we now talk about how it is utilized as a part of the connection of the A3P center. At the point when a client transfers a picture, it is taken care of as an information question picture.

The mark of the recently transferred picture is contrasted and the marks of pictures in the present picture database. To decide the class of the transferred picture, we locate its first m nearest coordinates. The class of the transferred picture is then computed as the class to which dominant part of the m pictures have a place.

On the off chance that no overwhelming class is found, another class is made for the picture. Later on, if the anticipated strategy for this new picture turns out right, the picture will be embedded into the relating picture class in our picture database, to refine future arrangement expectation. In our present model, m is set to 25 which is gotten utilizing a little preparing information set.

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 4, April 2016

VIII. METADATA-BASED CLASSIFICATION

The metadata-based characterization bunches pictures into subcategories under previously stated benchmark classifications. The procedure comprises of three principle steps. The initial step is to remove watchwords from the metadata connected with a picture. The metadata considered in our work are labels, inscriptions, and remarks. We recognize every one of the things, verbs and descriptive words in the metadata and store them as metadata vectors tnoun ¼ ft1; t2; . . . ; tig, tverb ¼ ft1; t2; . . . ; tjg and tadj ¼ ft1; t2; . . . ; tkg, where i, j and k are the aggregate number of things, verbs and descriptive words individually. The second step is to determine an agent hypernym (meant as h) from every metadata vector. We first recover the hypernym for every ti in a metadata vector in view of the Wordnet grouping and get a rundown of hypernym h ¼ fðv1, f1Þ, ðv2, f2Þ; . . .g, where v means hypernym and f indicates its recurrence.

For instance, consider a metadata vector t ¼ f"cousin","first steps", "infant boy"g. We find that "cousin" and "infant kid" have the same hypernym "child", and "initial steps" has a hypernym "activity". Correspondingly, we acquire the hypernym list h ¼ f(kid, 2), (activity, 1)g. In this rundown, we select the hypernym with the most noteworthy recurrence to be the delegate hypernym, e.g., "kid". On the off chance that that there are more than one hypernyms with the same recurrence, we consider the hypernym nearest to the most significant pattern class to be the delegate hypernym. For instance, in the event that we have a hypernym list h ¼ f(kid, 2), (cousin, 2), (activity, 1)g, we will choose "child" to be the agent hypernym since it is nearest to the pattern class "kids".

The third step is to discover a subcategory that a picture has a place with. This is an incremental system. Toward the starting, the principal picture shapes a subcategory as itself and the delegate hypernyms of the picture turns into the subcategory's illustrative hypernyms. At that point, we figure the separation between agent hypernyms of another approaching picture and each current subcategory. Given a picture, let hn, ha and hv indicate its delegate hypernyms in the metadata vectors relating to things, descriptive words and verbs, separately. For a subcategory c, Let hc n, hc an and hc v indicates its agent hynpernyms of things, descriptors and verbs, separately. The separation between the picture and the subcategory is figured as a weighted aggregate of the alter separation between relating pair of delegate hypernyms as appeared in Equation (1), where w indicates the weight and D signifies the alter separation,

$$Dist_m = Wn \,.\, D(h_n, h_n^c) + Wa \,.\, D(ha, h_a^c) + Wv \,.\, D(hv, h_v^c)$$

Note that wn þ wa þ wv ¼ 1, and wn > wa > wv. In Equation (1), we give the most astounding weight to the hypernyms of the things since things are nearest to the gauge classes. We consider the hypenyms of the modifiers as also critical as the descriptive words can refine the gauge criteria. At last, we consider the hypernymms of the verbs. As a matter of course, wn ¼ 0:5, wa ¼ 0:3 and wv ¼ 0:2.Next we check if the nearest subcategory has the separation esteem littler than a limit . Assuming this is the case, the new picture will be incorporated into to the subcategory and we overhaul the agent hypernyms of the subcategory by keeping the hypernyms with the most astounding recurrence. Something else, another subcategory will be built for this picture.

IX. CONCLUSION

We have proposed an Adaptive Privacy Policy Prediction (A3P) framework that helps clients mechanize the protection approach settings for their transferred pictures. The A3P framework gives a thorough structure to surmise protection inclinations in view of the data accessible for a given client. We additionally adequately handled the issue of chilly begin, utilizing social setting data. Our exploratory study demonstrates that our A3P is a down to earth device that offers huge upgrades over current ways to deal with protection.

REFERENCES

[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.

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 4, April 2016

[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] 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.
[5] 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.
[6] D. G. Altman and J. M. Bland ,"Multiple significance tests: The bonferroni method," Brit. Med. J., vol. 310, no. 6973, 1995.
[7] J. Bonneau, J. Anderson, and L. Church, "Privacy suites: Shared privacy for social networks," in Proc. Symp. Usable Privacy Security, 2009.
[8] 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.
[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.
[11] L. Church, J. Anderson, J. Bonneau, and F. Stajano, "Privacy stories: Confidence on privacy behaviors through end user programming," in Proc. 5th Symp. Usable Privacy Security, 2009.
[12] R. da Silva Torres and A. Falc~ao, "Content-based image retrieval: Theory and applications," Revista de Informatica Teorica e Aplicada, vol. 2, no. 13, pp. 161–185, 2006.
[13] R. Datta, D. Joshi, J. Li, and J. Wang, "Image retrieval: Ideas, influences, and trends of the new age," ACM Comput. Surv., vol. 40, no. 2, p. 5, 2008.
[14] J. Deng, A. C. Berg, K. Li, and L. Fei-Fei, "What does classifying more than 10,000 image categories tell us?" in Proc. 11th Eur. Conf. Comput. Vis.: Part V, 2010, pp. 71–84. [Online]. Available: http://portal.acm.org/citation.cfm?id=1888150.1888157
[15] 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.

BIOGRAPHY

HALAMMA T.B., Studying M.Tech. Computer Science and Engineering. She is studying in The Oxford College of Engineering, Bangalore, Karnataka, India. Her areas of interests are Cloud computing, mobile cloud, cloudsim, networking, wireless communications.

LAVANYA. S, Assistant Professor, Department of Computer Science and Engineering and she has Completed her M.S. in Software Engineering and presently working in The Oxford college of Engineering, Bangalore, karnataka, India. Her areas of interests are Software Engineering, Cloud computing, mobile cloud, cloudsim, networking, wireless communications.