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. 3, Issue 9, September 2015

An improved Privacy of User Data and Images on Content Sharing Sites using BIC

D. Priyadharshini[1], Smrina Das[2]

Assistant Professor, Dept. of Computer Science, Sree Narayana Guru College, Coimbatore, India[1]

M.Phil. Scholar, Dept. of Computer Science, Sree Narayana Guru College, Coimbatore, India[2]

ABSTRACT: Social Network is an emerging E-service for content sharing sites (CSS). It is emerging service which provides a reliable communication, through this communication a new attack ground for data hackers; they can easily misuses the data through these media. Some users over CSS affects users privacy on their personal contents, where some users keep on sending unwanted comments and messages by taking advantage of the users' inherent trust in their relationship network. By this privacy of the user data may be loss for this issue this paper handles the most prevalent issues and threats targeting different CSS recently. This proposes a privacy policy prediction and access restrictions along with blocking scheme for social sites using data mining techniques. To perform this, the system utilizes APP (Access Policy Prediction) and Access control mechanism by applying BIC algorithm (Bayesian Information Criterion).

KEYWORDS*:* Social media, CSS, Privacy Data, APP and Bayesian Information Criterion,

I. INTRODUCTION

Social Networking (SN) is one of the improving technological with hundreds of millions of people participating to swapping their content through Text, media like image, audio, video, etc. Social media (SM) become one of the most important parts of our daily life as it allows us to communicate with a group of people. It assists an exterior of self expression for users, and assists them to entertain and exchange content with other users through social media's providing E-Service. Some of the Social media are Friendster.com, Tagged.com, Xanga.com, Live Journal, MySpace, Facebook, Twitter and LinkedIn have developed on the Internet over the past several years. It provides a content sharing mechanism and remote the people across the world. Users of social media can define a personal profile and modify it as they wish this features allows by the SM. Through this SM users may engage with each other for various purposes, with business, leisure, and knowledge sharing. People use social networks to get in touch with further people, and create and contribute content that includes personal information, images, and videos. The service providers have admission to the content present by their users and have the right to progression collected data and share them to unauthorized. A very familiar service provided in SN is to produce proposition for finding new friends, groups, and events using mutual filtering techniques. The success of the SN based on the number of users it attracts, and cheering users to add more users to their circle and to share data with other users in the SN so the information will goes across the world [1]. End users are nevertheless often not aware of the size or nature of the spectators accessing their data and the sense of understanding created by organism among digital friends often leads to disclosures that may not be suitable in a public forum. Such an open accessibility of data exposes in SN, the users obtain a number of security and privacy risks. In spite of the fact that content sharing represents one of the important features of existing Social Network sites, Social Networks yet do not sustain any mechanism for collaborative executive of privacy settings for shared content [2]. Social Networking sites are used by a huge number of users all over the world. It provides different features to the customers like chatting, posting comments, image sharing, video chatting etc.

Users regularly sharing the data and images in SN by this happening the privacy of the images may lock with the un-wanted parties. Hackers can chop the images through these social media so the privacy of the user images may loss. Today, for every single quantity of content sharing sites like Facebook—every wall post, photo, status update, and video—the up loader must settle on which of his friends, group members, and other Facebook users should be

DOI: 10.15680/IJIRCCE.2015. 0309096

intelligent to access the content. As a result, the problem of isolation on sites like Facebook has received significant concentration in both the research society [3] and the mainstream media. Our goal is to improve the set of privacy controls and defaults, but we are restricted by the reality that there has been no in-depth study of users' privacy settings on sites like Facebook. While significant privacy disobedience and mismatched user expectations are likely to exist, the extent to which such privacy disobedience arises has yet to be quantified [4].

II. LITERATURE REVIEW

Peter F. Klemperer [5] 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 [6]. 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 [7] to robotically detect private images, and to facilitate privacy-oriented image search. It coalesce textual meta data images with assortment of visual features to facilitates 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) [8] 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 A3P-core 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 [1,9] 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 [10].

Usage of social media's increased noticeably in today world which facilitate the user to distribute their personal information like images with the other. This enhanced technology leads to privacy disobedience where the users are allocation the large volumes of images across additional number of peoples. To provide security for the information, mechanical explanation of images are introduced which aims to create the meta data information about the images by using the novel approach called Semantic interpret Markovian Semantic Indexing(SMSI) for repossess the images [11]. The proposed system automatically interpret the images using hidden Markov model and features are extorted by using color histogram and Scale-invariant feature transform (or SIFT) descriptor method. After interpret these images, semantic retrieval of images can be done by using Natural Language giving out tool namely Word Net for measuring semantic comparison of annotated images in the database. Experimental results make available enhanced retrieval performance when evaluate with the existing system.

III. PROBLEM DEFINITION

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 [12, 13]. 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 SYSTEM

Some users over CSS influence user's privacy on their private contents, where some users keep on distribution superfluous comments and messages by attractive advantage of the users' intrinsic trust in their connection network.

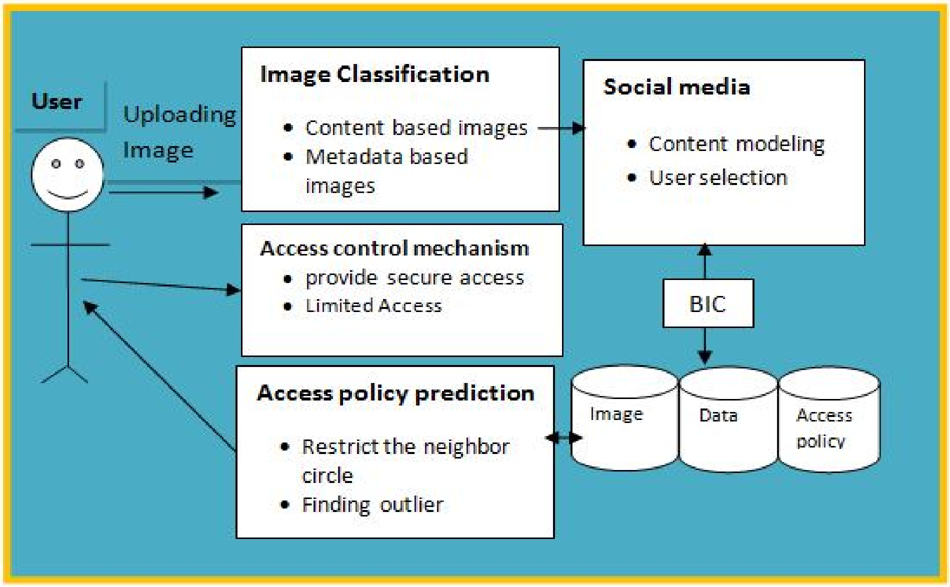


Figure 1: System Architecture

The overall architecture of the proposed work has given in figure 1.0. This paper switches the most widespread issues and threats objective different CSS freshly. In CSS privacy is frequently a key apprehension by the users. Because millions of people are willing to interrelate with others, it is also a new harass ground for image misuses. They are dispersion the images and contents. This paper will demonstrate and argue the most widespread issues and threats targeting different CSS today. And finally finds the just the thing privacy policy scheme for that privacy. This proposition a privacy policy forecast and access boundaries along with overcrowding scheme for social sites using data mining techniques. This helps to detect and defend distrustful activates, which violates user's privacy in CSS by making an allowance for the following parameters, i) Text annotation, which emerge in the uploaded contents. ii) Image and policy descriptions iii) Detection of superfluous commends and. To perform this, the system utilizes APP (Access Policy Prediction) and Access control mechanism by applying BIC algorithm (Bayesian Information Criterion).

a. Access Policy Prediction

Accessing the personal data in E-service make available an information distribution diagonally the world and at the same time it not working the privacy of the user data. Access policy is for retrieving the data or image in the network. By this kind of right of entry privacy may loss. For this problem the user of the social media compute the normalized and prejudiced average of the ratings of the users in the district. User have to confine the neighbor circle so un-wanted may not influence the data [13, 14]. User have to envisage the neighbor circle and provide a limited admission technique they have to choose 1) what information one disclose about oneself, and (2)who can access that information. Fundamentally, when the data is collected or investigate without the knowledge or consent of its owner, privacy is violated.

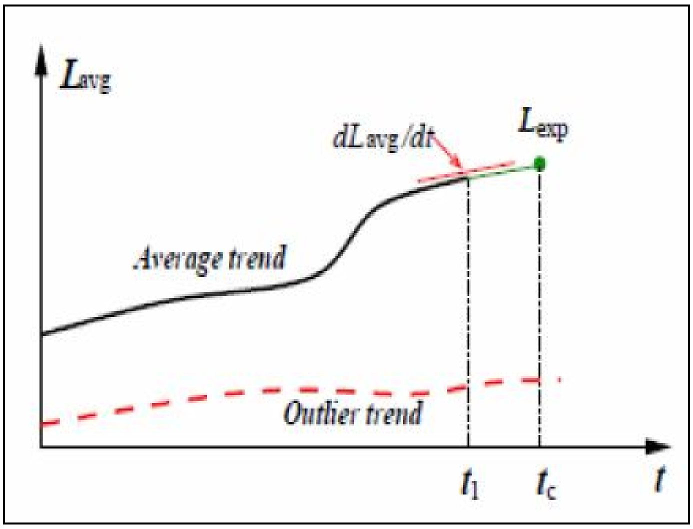


Figure 2: Outlier Prediction policy

When it comes to the usage of the data, the owner should be knowledgeable about the principle and purpose for which the data is organism or will be used and to provide a partiality. They have to set the level of regular to predict using (1). This shows the average level of predict policy which provides the result of strictness level of policy Pi, and Np is the total number of policies. By decision this we may get the ***Outlier*** so we can easily investigate the misuse party (See 2.0).

b. Access control mechanism

Access control in the shared environment is one of the essential one. To supply a secure access we have to limit the un-authorized user in these networks. Access control mechanism (ACM) is one of the privacy conserve one. ACM permit users to oversee access to information controlled in own spaces, users, unhappily, have no control over data be inherent in outside their spaces [15, 16]. For example, Facebook allows label users to eliminate the tags associated to their profiles or report contravention asking Facebook managers to eliminate the contents that they do not want to split among the public.

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. 3, Issue 9, September 2015

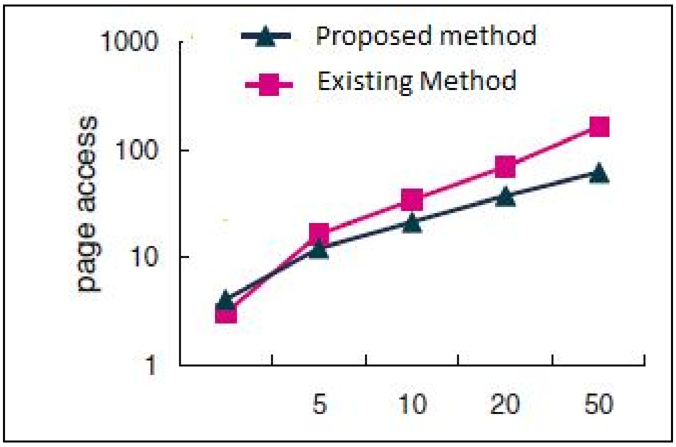


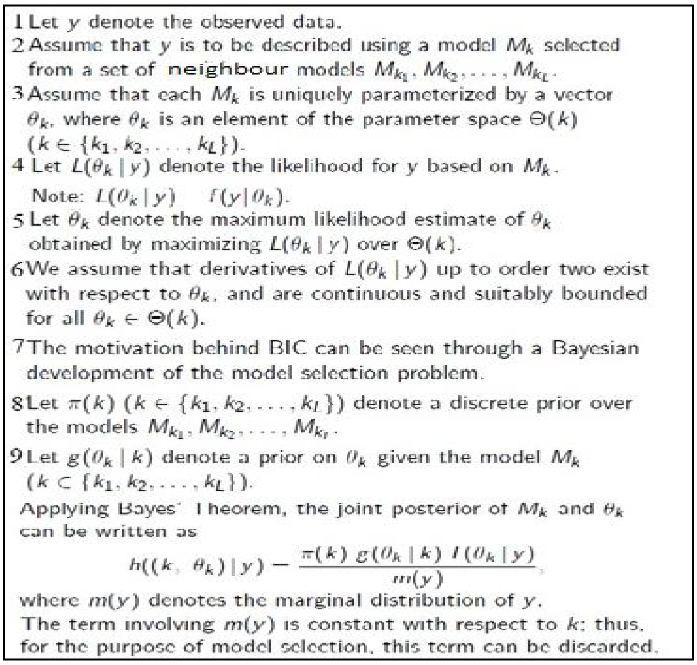
Figure 3.0: Difference between Existing and Proposed

This shows the diverse between existing and the proposed system (see figure 3.0). In the proposed system the access of the pages were limited when compared to existing system. Access control is by provided that access rights in a SN are limited to few basic constitutional rights, such as read, write and play for media content. This based type of approach which generates access-control policies from photo administration tags. Every photo is integrated with an access grid for mapping the photo with the participant's friends. The contestant can select a suitable partiality and access the information. Photo tags can be categorized as directorial or forthcoming based on the user needs.

c. Proposed Algorithm:

Bayesian information criterion was introduced by Schwarz (1978) as a participant to the Akaike (1973, 1974) information criterion. Schwarz derived BIC to serve as an asymptotic rough calculation to a conversion of the Bayesian posterior probability of a contender model[17]. In large-sample scenery the en suite model favored by BIC if possible communicate to the competitor model which is a posteriori most probable; i.e., the model which is provide most plausible by the data at hand.

Algorithm:



1 Let y denote the observed data.

2 Assume that y is to be described using a model M_k selected from a set of neighbour models $M_{k_1}, M_{k_2}, \ldots, M_{k_L}$.

3 Assume that each M_k is uniquely parameterized by a vector θ_k, where θ_k is an element of the parameter space $\Theta(k)$ $(k \in \{k_1, k_2, \ldots, k_L\})$.

4 Let $L(\theta_k \mid y)$ denote the likelihood for y based on M_k.

Note: $L(\theta_k \mid y) \quad f(y \mid \theta_k)$.

5 Let θ_k denote the maximum likelihood estimate of θ_k obtained by maximizing $L(\theta_k \mid y)$ over $\Theta(k)$.

6 We assume that derivatives of $L(\theta_k \mid y)$ up to order two exist with respect to θ_k, and are continuous and suitably bounded for all $\theta_k \in \Theta(k)$.

7 The motivation behind BIC can be seen through a Bayesian development of the model selection problem.

8 Let $\pi(k)$ $(k \in \{k_1, k_2, \ldots, k_l\})$ denote a discrete prior over the models $M_{k_1}, M_{k_2}, \ldots, M_{k_l}$.

9 Let $g(\theta_k \mid k)$ denote a prior on θ_k given the model M_k $(k \subset \{k_1, k_2, \ldots, k_L\})$.

Applying Bayes' Theorem, the joint posterior of M_k and θ_k can be written as

$$h((k, \theta_k) \mid y) = \frac{\pi(k)\, g(\theta_k \mid k)\, L(\theta_k \mid y)}{m(y)},$$

where $m(y)$ denotes the marginal distribution of y.

The term involving $m(y)$ is constant with respect to k; thus, for the purpose of model selection, this term can be discarded.

DOI: 10.15680/IJIRCCE.2015. 0309096

In Bayesian applications, pair wise comparisons between models are over and over again based on Bayes factors. Presumptuous two candidate models are regarded as equally probable a priori, a Bayes factor correspond to the ratio of the posterior likelihood of the models. The model which is a posteriori most likely is determined by whether the Bayes factor is less than or greater than one [17].

V. CONCLUSION

Social network is an upgrading media for information sharing through internet. It provides a content sharing like text, image, audio, video, etc… With this emerging E-service for content sharing in social sites privacy is an important issue. It is an emerging service which provides a reliable communication, through this a new attack ground from an un-authored person can easily misuses the data through these media. For this issue our proposed systems use the BIC algorithm to classify the attackers and the users with the help of the Access Policy Prediction and Access control mechanism. These provide a privacy policy prediction and access restrictions along with blocking scheme for social sites and improve the privacy level for the user in social media.

REFERENCES

[1]. S.Thiraviya Regina Rajam1 and Dr. S.Britto.Ramesh Kumar, “SOCIAL NETWORK SERVICES: ANOVERVIEW”.
[2] H. Sundaram, L. Xie, M. De Choudhury, Y. Lin, and A. Natsev,“Multimedia semantics: Interactions between content andcommunity,” Proc. IEEE, vol. 100, no. 9, pp. 2737–2758, Sep. 2012.
[3] S. Ahern, D. Eckles, N. Good, S. King, M. Naaman,and R. Nair. Over-Exposed? Privacy Patterns and Considerations in Online and Mobile Photo Sharing.CHI, 2007.
[4] Sangeetha. J ,Kavitha. R, “An Improved Privacy Policy Inference over the Socially Shared Images with AutomatedAnnotation Process”
[5]. Peter F. Klemperer, Yuan Liang, Michelle L. Mazurek, “Tag, You Can See It! Using Tags for Access Control in Photo Sharing”, Conference on Human Factors in Computing Systems, May 2012.
[6]. A. Kapadia, F. Adu-Oppong, C. K. Gardiner, and P. P. Tsang, “Social circles: Tackling privacy in social networks,” in Proc. Symp. Sable Privacy Security, 2008.
[7]. SergejZerr, Stefan Siersdorfer, Jonathon Hare, Elena Demidova , I Know What You Did Last Summer!:Privacy-Aware Image Classification and Search , Proceedings of the 35th international ACM SIGIR conference on Research and development in information retrieval, 2012
[8]. Anna CinziaSquicciarini, “Privacy Policy Inference of User-Uploaded Images on Content Sharing Sites”, IEEE Transactions On Knowledge And Data Engineering, vol. 27, no. 1, January 2015.
[9]. Ms.B.Hema and Ms.S.Sivagami, “Survey on secure and time confined image sharing on websites”.
[10] Anna C. Squicciarini, Mohamed Shehab, Federica Paci “Collective Privacy Management in Social Networks”.
[11] Sangeetha. J 1, Kavitha,“An Improved Privacy Policy Inference over theSocially Shared Images with AutomatedAnnotation Process”.
[12]. Privacy Policy Inference of User-UploadedImages on Content Sharing SitesAnna CinziaSquicciarini, Member, IEEE, Dan Lin, SmithaSundareswaran, and Joshua Wede.
[13] K. Strater and H. Lipford, “Strategies and struggles with privacyin an online social networking community,” in Proc. Brit. Comput.Soc. Conf. Human-Comput. Interact., 2008, pp.111–119.
[14] A. C. Squicciarini, S. Sundareswaran, D. Lin, and J. Wede, “A3p:Adaptive policy prediction for shared images over popular contentsharing sites,” in Proc. 22nd ACM Conf. Hypertext Hypermedia,2011, pp.261–270.
[15] P. Klemperer, Y. Liang, M. Mazurek, M. Sleeper, B. Ur, L. Bauer,L. F. Cranor, N. Gupta, and M. Reiter, “Tag, you can see it!: Usingtags for access control in photo sharing,” in Proc. ACM Annu.Conf. Human Factors Comput. Syst., 2012, pp. 377–386.
[16] C. A. Yeung, L. Kagal, N. Gibbins, and N. Shadbolt, “Providingaccess control to online photo albums based on tags and linkeddata,” in Proc. Soc. Semantic Web: Where Web 2.0 Meets Web 3.0 atthe AAAI Symp., 2009, pp. 9–14.
[17] Joseph E. Cavanaugh, “Bayesian Information Criterion” Sep 25, 2012.
[18] Shivaji Mutkule1, Praful Sonarkar2 and Meghana Nagori3, “Establishing Effective Connectivity in Brain usingDynamic Bayesian Network”.