IMPROVED PRIVACY POLICY PREDICTION OF USER UPLOADED PROFILE IMAGES IN SOCIAL MEDIA SITES

S. Mayil[1], M. Vanitha[2]

[1]Research Scholar, PG and Research Department of Computer Science,
J.J. College of Arts and Science (Autonomous), Pudukkottai, TamilNadu, India.
Email id:mayilma@yahoo.co.in

[2]Assistant professor, Department of Computer Applications,
Alagappa University, Karaikudi, TamilNadu, India.
Email id:mvanitharavi@gmail.com

***Abstract*— Online social networking has become one of the most popular activities on the Internet. Over the years, all online activities have accumulated a huge amounts of data. The data validity attracts many for discovery of new knowledge and multiple analysis based on the needs of the parties. Recently announced events, a user's inadvertent exchange of personal information and Image sharing has become a major problem in maintaining user privacy. Thus it becomes evident for usage of tools to control access to user shared contents. Image sharing are used more in a user's social discoveries of groups, identifying new partners, understanding peers and social environment. Content sharing can lead to private information disclosure, while aggregate information may cause accidental exposure and misuse of personal information. This paper proposes an Improved Privacy Policy (I3P), where users define their privacy settings of image content. The proposed solution is based on a framework that can be automatically associated to such a policy. By using a predictive algorithm, automatic categorizations of images can be generated based on user's social characteristics.**

Keywords- Improved Privacy Policy Prediction (I3P), I3P Core, I3P Social.

I. INTRODUCTION

Social networking services (SNS), such as Face book, LinkedIn or Orkut, are today's dominant services on the web. They cover a wide range of users in social, educational and national planes. They allow users with limited technical ability to publish personal information and are easy to communicate. In general, the online social network (OSN), is a digital representation of a subset of the people or institutions whose participants are registered in the physical world. The social network participants and their relationships can be modeled as a chart. Social networking services are widely accepted like SMS platforms and the socialization has attracted not only loyal users, who try to add value to the community, but also certain unfavorable parties.

Memberships in OSN, creation of profiles, motivations and applications provided by these services is designed to communicate easily with selected contacts for professional or personal purposes. OSNs installed for managing career or business are more serious like XING or LinkedIn. Any published content is on the professional ethics, where members know the impact of such publications. Personal usage of social media involves sharing of more personal information such as contact information, personal photos or videos. Other members share images that can be tagged ("tagged") and automatically create respective profile links. The application of online social networking (OSN) is the most commonly used data exchange and has been increasing in recent years and become an indispensable part of daily lives. Real-time communication (MSN), Internet telephony (Skype), offline communication, private information (YouTube) and blogs are used regardless of their physical location. National Bureau of Statistics sites include Face book, MySpace and Twitter are familiar to many people. Travel, business, school and so on. They make it easier for social groups, families and friends to maintain social relationships in a more comfortable and affordable manner than traditional telephone or e-mail.

Despite these attractive features, the privacy of user's data is used for malicious activities, such as private data without access to private data, unauthorized private data, and analysis of owner risky data. Users on OSN applications (such as Face book) are vulnerable and lead to compromising real names and personal information. The result is that the National Bureau of Statistics maintains a high degree of privacy for efficiency and data sharing systems.

II. LITERATURE REVIEW

Jemal Abawajy et al., in their comprehensive investigation social networks highlighted recent development in risks due to attacks and the need for data privacy. This paper researches the presence of various types of attacks on privacy of social networks data. Current preservation technologies collect data from publications indexing the amount of information provided by anonymous information and social networks as well as challenges faced with new research directions. The survey helped readers understand threats to protect privacy and security, vulnerabilities in privacy publishing data and observe common problems analyzing high-level frameworks in social network threats. The work also presented a model to quantify and classify the background of the privacy information that can be used by the opponent to break into social network data [1].

According to Prajakta Tambe et al., Online social networking (OSN) is becoming more and more important in daily lives. Statistics show that 74% of Internet users are involved in social networking. Unfortunately, most of the users do not know the threat and vulnerability of OSNs. The problems can be resolved by data removal, where the process conceals sensitive information with false data. The system uses alternative methods to disinfect garbled keywords, as nouns and verbs provide information from words. They are treated as keywords and words, and the rest are treated as functional words. The keyword are processed using a native programming language (API) POSTAGGER (word class) natural language processing of Stanford (NLP) for disinfection [2].

Roman Schlegel et al. proposed Encryption for social networking applications (PPLSS). The salient features of PPLSS were (1) allowing a group of friends without having any third party or any leaked location information to any server or group of people outside the group to share their exact location, (2) to achieve a low processing by allowing the user to receive the exact location of friend's communication without the need for communication between the user and multiple rounds of communication between the user and the server, (3) through a design structure to provide an efficient query processing index ORE , (4) program support for dynamic update location and (5) providing a set of friends to specify one of the users to prepare the maximum distance within the customized privacy protection of friends [3].

Dongsheng Li et al. recommended a system based on user groups and online social community users to protect privacy. In this system, the user groups with different interest groups interacts with servers that use a particular pseudo-user, thus hiding personal data of an individual from others in the server. They also recommended privacy protection of a group of users in a referral process using protocols and strategies. They implemented their prototype on mobile devices and desktop computers using real-world data and the evaluation showed that their YANA could effectively provide high quality protection of users' privacy while getting recommended with energy efficiency. Also their experimental results showed that the privacy protection with YANA achieved much better quality recommendations and were effective in maintaining online social community user privacy interests [4].

Varsha Bhat Kukkala et al. studied privacy issues and restrictions on confidential information access in networked data. Networks capture relationships such as trust, hostility, sexual contact, which are examples of sensitive networks. They showed that protocols used an arithmetic black box supporting arithmetic operations equal to an extension of existing validated security. A multi-party calculation protocol constructed a secure unmarked graph of an isomorphic distributed a set of n random parts. It was showed that the proposed the hybrid model of the FabB protocol was safe. The agreement studied all aspects of individual behavior while ensuring the privacy of sensitive data. Anonymous data was released before publicly releasing sensitive data. The work was naive and did not use trusted third parties in a distributed network. The multi-party computing technology was also implementable for specific anonymous network protocols [5].

III. METHODOLOGY

III.A. Preliminary Notions

Users can express their privacy preferences through a social privacy policy. The privacy policy is defined. This methodology is inspired by popular content sharing sites (eg Face book, Picasa, Flicker), but the actual implementation relies on the infrastructure and implementation of specific content management in social media sites.

III.B. System Overview

The I3P system consists of two parts: I3P core and society. The total data flow is as follows. When the user uploads the image, the image is first sent to the core of the I3P. Core I3P then classifies images and determines whether it is necessary to call I3P-society module. In most cases, the I3P's core forecasting policy is based directly on the historical performance of the user. I3P core I3Psocial is called if: (i) the user does not have sufficient data to predict the type of the file uploaded or (b) the I3P core detects the user follows self-privacy practices and if the following is true: Provide more social networking activities (add new friends, new messages, personal information, etc.) along with the latest changes in the community. In the First case, it would be useful to inform the user of the social group's ultimate privacy practices similar to the background of the user. The I3P brings together social groups with similar social backgrounds and privacy preferences for social groups with

continuous monitoring. When calling the I3P-society, social groups can automatically identify the user and return information about the core group I3P to predict information and the final plan will be displayed to the user. If the user is fully satisfied with the planned policy, it is accepted, else the user can choose to view the policy. The current strategy is stored in the strategy library system to predict future policy changes.

III.C. Privacy In Social Networks

The design goal is to provide a platform to meet user's privacy expectations on social networking sites by ensuring that users can only provide user data to other users through the same platform that can be seen through the standard Web interface.

III.C.1 User Expectations

The privacy expectations in social networking are based on relationships. Typical social networking supports privileged access to friends and networks.

III.C.2. Friends.

Friendship is a defining feature of social networking sites, and friends have access to personal data. Friends need to be recognized from both ends. Sometimes the privilege may be extended to the second or third degree connections.

III.C.3. Networks.

Social networks also support member access in the network. Access control in Bebop and Face book is related to admission. Alternatively, a custom area may be considered on the network and privacy control may be associated with the selected location. For example, Friendster users can limit profile to some mainland's popularity.

III.C.4. Public visibility.

The site defines a subset of the configuration file (such as user name and affiliation), by default, search and visible recognition. Most sites also allow users to relax or enhance the definition of public information.

III.D. I3P-CORE

There are two main components in the I3P core: (i) in the image classification and (ii) the adaptive prediction strategy. For each user, their photo is based on the first sort of content and metadata. Then, each image category of the privacy policy is analyzed for predictions. The two-step approach is more suitable for policy advice on the commonly used methods of data mining in a single step to implement a joint review of the characteristics and image of the policy. When a user loads a new image, the user looks forward to a suggested policy. The two-step approach allows the system to use the first step, the new image is sorted and the candidate set image follows the policy recommendations. The extraction method is a single stage, it will not be able to find the correct class of new images because their classification criteria requires the aforesaid imaging characteristics of the policy and the new image of the policy is not published. Moreover, in a single classification leading the image and the characteristics of the policy, the system is highly dependent on the specific grammar of the combination. If a change is supported by all the learning models the introduction policy will have to change.

- Sort images based on content and metadata. Then, each image category of the privacy policy is analyzed for predictions.
- In one of the two stages of the proposed system, one major policy is to use the data mining methods in the image feature extraction and policy, step by step along with the application.
- By implementing a two-step approach, the system initially categorizes the images and then looks for and specifies a set of correct policy recommendations. This practice is not in the mining may be in a stage, because the policy has not yet been announced.
- In order to make the system of independent political specific grammar, it is essential to achieve a two-stage approach. This also helps to separate the learning patterns when there is a policy change.

III.E. Algorithm Steps

```
User (U) uploads an image (I)
It is sent to I3P core
    If I3P core classifies I Then
        predict policies (P) for (U)
     else
        I3P social is called
            social group (SG) of the user is identified
    end if
```

(P) is shown to the user
if (U) is satisfied with (P) Then
(P) is Accepted(A) by (U)
end if. //

III.F. I3P-Social

The I3P-Society uses a mechanism to generate multiple inferences using key information about the user's social context and their general attitude towards privacy. As mentioned above, I3Psocial will be called by the I3P core in two cases. One is when the user is a novice on the site and there is not enough stored images for the I3P core to infer meaningful and customized strategies. The other case is when the system detects privacy changes in the user's social circle which may be of interest to the user and adjust privacy settings correspondingly. The social context of the type considered is proposed by the I3P community, and then presented to the policy recommendation process.

III.G. Improved Policy Prediction

The policy prediction algorithm provides a reference to the image of a new user's forecast growth policy. More importantly, the planned policies reflect any changes that occur in a user's privacy. The forecasting process consists of three main phases: strategy (i) normalization; (ii) mining policy; and (iii) forecasting policy. The normalization strategy is a simple set of rules for the decomposition in which the atomic data component (D) is a unique set of user policies.

IV. EXPERIMENTAL RESULTS

There are two main components in the I3P core: (i) in the image classification and (ii) the adaptive prediction strategy. For each user, the photo is based on the first sort of content and metadata. Then, each image category of the privacy policy is analyzed for predictions. The two-step approach is more suitable for policy advice on the commonly used methods of data mining in a single step to implement a joint review of the characteristics and image of the policy. When a user loads a new image, the user looks forward to a suggested policy. The two-step approach allows the system to use the first step, the new image is sorted and the candidate set image is found based on policy recommendations. The extraction method is one stage, it may not be able to find the correct class of new images because their classification criteria require two imaging characteristics of the policy, and the new image of the policy may not have been published. In a single classification of the image and characteristics of the policy, a system may be highly dependent on specific grammar of the combination. If a change is supported by all the learning models, then the introduction of a policy will have to change.

IV.A. Image Classification

Content-based categorization is based on a method that is similar to an efficient and accurate image categorization. The classification algorithm compares the signatures of the images defined based on the quantized transformation and disinfection of the Bohar version, image frequency information and the spatial information of the color, size and texture of the image. A few of the coefficients are selected to form the signature of the image. The similarity criteria are selected from the image including texture, symmetry, shape, and color of the image.

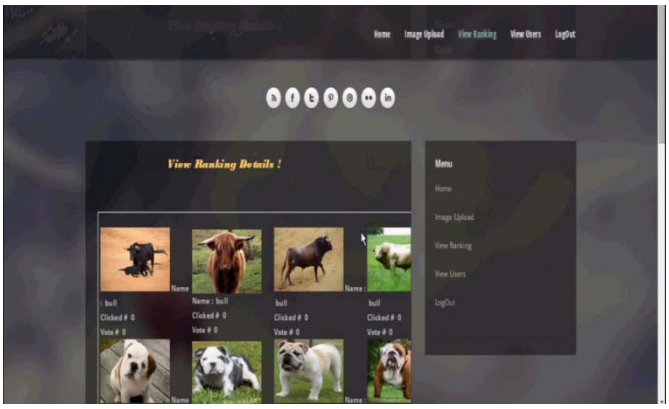

Fig.1. Image Classification

The user loads the image; it is processed as a query for the image input. The signature of the newly loaded image is compared with the signature of the image in the current image in the database. The uploaded images in the class are then calculated as the classes of most of their **m** images. If there is no ruling class, a new class of images is created. Then, if the new image plan policy is correct, the image is inserted in the image category correspondingly in the image database B for improved policy prediction

By collecting the image data to predict the political image and comparing it to an algorithmic benchmark, without considering the social context, the proposed method is similar to the privacy settings of the social group. Using the baseline method regardless of the user's personal privacy tilt in images results in the best accuracy.

Users maintain a more consistent policy and the proposed algorithms can be effectively learnt. Looking for images and based on the image content found in each user privacy information on a site to share the fixed image the proposed method is a new technique in social policy recommendations, called by the I3P I3P kernel. The number of users' social networks is huge and can join a large number of social groups and may spend too much time comparing the attributes of the social context of the various social groups with frequent patterns of users.

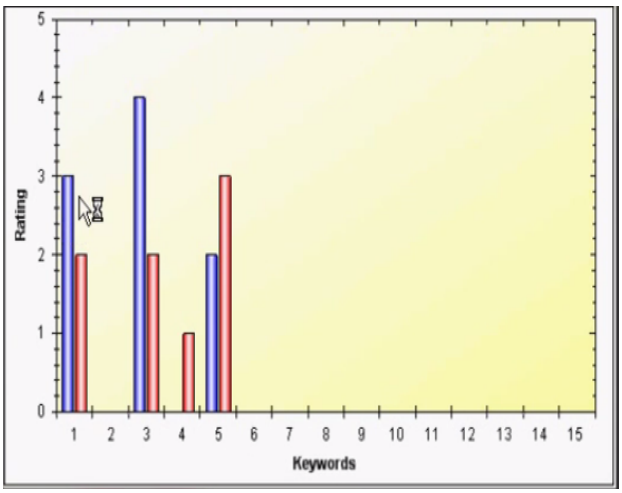

Fig.2. Performance Evaluation of Keyword Ranking

V. CONCLUSION

The proposed Privacy Policy Improved Forecast (I3P) helps users automate their configuration to load image privacy. Privacy Preferences. The I3P repository provides a comprehensive framework for inferring content sharing for specific users . It can also effectively solve problems in the use of information in a social environment. The proposed methods experimental results show that I3P is a useful tool for providing significant improvements in user privacy on social media sites. Software filters unwanted social networking messages. GUI filtering designs based on user actions in OSN behavior and reputation can help OSN audit mechanism for users. Also a set of each short text message is automatically assigned by extending the text classification of Machine Learning (ML) technology based on its content category. There is also flexibility to specify the Filtering Rules (FR), whereby the user can indicate which content should not be displayed. RF can support a variety of filtering criteria according to the user being combined and customized. Thus this paper has proposed and demonstrated a new technique for preserving user privacy in a public domain like social media sites.

REFERENCES

[1] Jemal Abawajy, Mohd Izuan Hafez Ninggal and Tutut Herawan by “Privacy Preserving Social Network Data Publication”, IEEE Transaction, (2016).
[2] Prajakta Tambe, Deepali Vora by “Data Sanitization for Privacy Preservation on Social Network”, International Conference on Automatic Control and Dynamic Optimization Techniques (ICACDOT), (2016).
[3] Roman Schlegel, Chi-Yin Chow, Chi-Yin Chow, and Duncan S. Wong by “Privacy-Preserving Location Sharing Services for Social Networks”, IEEE Transactions on Services Computing, (2016).
[4] Dongsheng Li, Qin Lv, Li Shang, Ning Gu by “Efficient Privacy-Preserving Content Recommendation for Online Social Communities”, ELSEVIER, (2016).
[5] Varsha Bhat Kukkala, Jaspal Singh Saini, S.R.S. Iyengar “Secure Multiparty Construction of a Distributed Social Network”, ELSEVIER, (2017).
[6] Pares-Pulido and Isaac Agudo by” LockPic: Privacy Preserving Photo Sharing in Social Networks” Carlos,DPM and QASA 2015, LNCS 9481, pp. 281–290, (2016).
[7] Dixit Ulhas and Jive Mayur by “Preserving and Controlling Privacy on sharing of Photos over Social Network Site”, Vol. 4, Issue 3, (2016).
[8] Balkirat Kaur and Malcolm Blow by, “Authenticity of Digital Images in Social Media” ,(2016).
[9] Imad S. W. Khufash and Hebah H. O. Nasereddin by “New Technique to Protect the Privacy of Images in Social Network by Using Hash Algorithm & Least Significant Bit”, International Journal of Advanced Research in Computer Science and Software Engineering 5(11),(2015).
[10] Xingliang Yuan and Xinyu Wang by “Enabling Privacy-preserving Image-centric Social Discovery”, 2014 IEEE 34th International Conference on Distributed Computing Systems, 1063-6927/14 $31.00 ©IEEE (2014).
[11] Sowmya V., Sripriya N. by “Searching Image Privacy Rules in Content Sharing Sites on Social Network”, Imperial Journal of Interdisciplinary Research (IJIR) Vol-2, Issue-4, ISSN: 2454-1362,(2016).
[12] Ming Li, Ning Cao , Shucheng Yu and Wenjing Lou, by “FindU: Privacy-Preserving Personal Profile Matching in Mobile Social Networks” ©IEEE (2011).

[13] Weiwei Sun, Jiantao Zhou, Ran Lyu, Shuyuan Zhu by "Processing-Aware Privacy-Preserving Photo Sharing over Online Social Networks" October 15–19, 2016, Amsterdam, The Netherlands.oc (2016).
[14] Jinyuan Sun, Xiaoyan Zhu, and Yuguang Fang, by A Privacy-Preserving Scheme for Online SocialNetworks with Efficient Revocation, IEEE INFOCOM (2010).
[15] Abhilasha Singh Rathor, Pawan Kumar Mishra by "Social Networking Websites and Image Privacy" IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 10, Issue 6, PP 59-65,(2013).
[16] Kundan Shewale, Sachin D. Babar by "An Efficient Profile Matching Protocol Using Privacy Preserving In Mobile Social Network ",Elsevier, (2016).
[17] Weiwei Sun, Jiantao Zhou, Ran Lyu, Shuyuan Zhu by Processing-Aware Privacy-Preserving Photo Sharing over Online Social Networks",(2016).
[18] M. Muthubrindha, Dr. A. Valarmathi by "Privacy Based Image and Comment Sharing on Online Social Networks Based on Short Text Classification", IJARCSSE, (2016).
[19] Lin Yuan, Pavel Korshunov, and Touradj Ebrahimi by "Privacy-Preserving Photo Sharing based on a Secure JPEG",(2013).