Scholars Journal of Engineering and Technology (SJET) **ISSN 2347-9523 (Print)**
Abbreviated Key Title: Sch. J. Eng. Tech. **ISSN 2321-435X (Online)**
©Scholars Academic and Scientific Publisher
A Unit of Scholars Academic and Scientific Society, India
www.saspublisher.com

A Review on Various Techniques of Sharing Photo on Online Social Networks

Bhavisha Rajput[1*], Mrs. Minu Choudhary[2]
[1]Dept. of Computer Science and Engineering, Rungta College of Engineering and Management Bhilai, Chhattisgarh, India
[2]Dept. of Information Technology, Rungta College of Engineering and Management, Bhilai, Chhattisgarh, India

Review Article

***Corresponding author**
Bhavisha Rajput

Article History
Received: 08.11.2017
Accepted: 07.12.2017
Published: 30.12.2017

DOI:
10.21276/sjet.2017.5.12.1

Abstract: At the present days people share many private images on social networking sites which needs maintaining privacy. Privacy is needed to prevent the misuse of such images. For preserving these images secure different privacy settings are needed. If a tool is granted to the user which will bring him set privacy easily, this will decrease his task. For addressing this requires various techniques are proposed. In this paper, some of the privacy recommendation techniques are discussed. These techniques used to recommend the privacy to user for images that the user share on online social networking site. In order to recommending such privacy on photo sharing on social media, user profile information and properties of images are used. Tags related to images and visual properties also essential to categories images.

Keywords: Privacy Policy, Online Social Network, Facebook, Privacy Recommendation, Security

INTRODUCTION

Social networking sites have become a very important part of our day-today life. Online social networks (OSNs) such as Facebook, Google and instagram are implicitly designed to make able people to be the part of personal and public information and make people to connect with friends, co-workers, persons having like-position, family, and even with strangers socially. To keep safe (out of danger) user’s personal information, way in control has become a chief thing point of Online Social Networking sites.

On the other hand, it becomes everlasting record once some photo or image is posted or uploaded on social network. Late consequences can be insecure, people may use it for various unexpected intentions. For example a posted information may disclose the mafia relationship of any celebrity.

A user profile usually involve information in order to the users work history birthday, sex, residence, interests, education, travel information, etc. other than this be in touch information also. As well as users can upload the picture and tag that picture to other people for all that they are willing or not willing to be part of uploaded image or content. At the same time other people are tagged, the situation becomes more complicated. The user uploaded the image is totally not known of the consequences that arise for the person which is included in tagging or uploading of images and contents. At present nobody can stop such unavoidable circumstances. We need to have a control over such activities to reduce the risks of photos being tagged or uploaded. In place of enforce restrictions over such incidents or increasing security on social networking sites like Facebook and Instagram which help for encouraging people to get into such things more.

Lots of time user is unwilling get tagged or brought to light without his permission. Here the question arises that is it violation if we share images without taking a permit from all the people who are involved in that particular image? The answer of this question we need to illustrate the privacy and security problem over the social sites.

Whenever an image is shared on OSN’s, it includes everybody’s security, which can be put on risk if the proper approvals are not sought. We need to impose maximum level of privacy and security of the content being uploaded on social sites. In such manner while using the online social networks one can perceive desired level of confidence and security. He/she can with confidently make use of social sites without concern or photos being shared in insecure and unauthorized way. Desired level of privacy and security is a most important thing for a user using online social sites.

The current architecture and implementations of social networking sites, either user will alone because highly enforced the security constraints else will be impacted by several security threats because of low security procedures. Few authors studied about the security challenges because of lack of joint or collaborative control over the photo being shared across the online social sites.

To reduce this or to completely avoid this they have suggested social networking sites like Facebook, Instagram to make use of multi-party privacy model to enhance privacy. Therefore, it needs to be mutual acceptable policy to grant access for an image when multiple user are included. For security purpose user might need to make a group in which they can grant access for their uploaded photos. Exposure policy should be well-defined as the whole group of users where an image can be accessed properly when a single user is involved and the privacy policy can be defined as the group of users/friends who can have a complete access of the uploaded images.

Hence these two safety policies are used to illustrate the overall audience or group of users or group of friends who can be given direct access to uploaded image. Whereas before establishing this there should be a proper procedure of defining these groups. For this the facial recognitions can be used. Most of the times the people found in the co-photo which are uploaded by close friends. So face recognitions engines are trained for identifying the friends in social circle. Face Recognition engines with more accuracy rates needs large number of test data/samples specific to a person but most of the times it is not possible.

Most of the times, the users who care about the privacy and security mostly restrict themselves from uploading the images but if these people are provided with proper privacy preserving techniques then they can post photos without bothering. Whatever for the architecture and applications of current social networking sites, whether used alone because of the latest security restrictions enforce different security threats will be affected due to a major security mechanisms. In this paper, few authors study on security issues due to the lack of joint control or cooperative on the images that have been shared through social networking sites on the World Wide Web.

LITERATURE SURVEY

Anna Cinzia Squicciarini [1] proposed with the increasing volume of images users share through social sites, 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, we propose an Adaptive Privacy Policy Prediction (A3P) system to help users compose privacy settings for their images. We examine the role of social context, image content, and metadata as possible indicators of users' privacy preferences. Author proposes a two-level framework which according to the user's available history on the site determines the best available privacy policy for the user's images being uploaded. Our 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 users' social features. Over time, the generated policies will follow the evolution of users' privacy attitude. We provide the results of our extensive evaluation over 5,000 policies, which demonstrate the effectiveness of our system, with prediction accuracies over 90 percent. An Adaptive Privacy Policy Prediction (A3P) system that helps users automates the privacy policy settings for their uploaded images. The A3P system provides a comprehensive framework to infer privacy preferences based on the information available for a given user. We also effectively tackled the issue of cold-start, leveraging social context information. The experimental study proves that our A3P is a practical tool that offers significant improvements over current approaches to privacy.

Peter F. Klemperer [2] found that find that (a) tags created for organizational purposes can be repurposed to create efficient and reasonably accurate access-control rules; (b) users tagging with access control in mind develop coherent strategies that lead to significantly more accurate rules than those associated with organizational tags alone; and (c) participants can understand and actively engage with the concept of tag-based access control. Tag-based rules are promising for use in an access-control system. Organizational tags can be repurposed to create reasonable access-control policies, and when participants actively create tags for access control, policies based on these tags are yet more accurate. Participants are able to suggest and engage actively with tag-based rules.

P.Srilakshmi [3] proposed that online social networks help people to socialize with the world. But users should be aware of threats that can be faced due to lack of proper privacy settings. In this paper a novel method for collaborative sharing of data in OSNs is discussed as well as a method to resolve privacy conflicts that can occur while multiple persons share a data. Evaluation results show that privacy risk and data sharing loss are minimized in this approach. Various websites offer services such as uploading, hosting, and managing for photo-sharing (publicly or privately). These functions are provided by websites and applications that facilitate the upload and display of images. The term may even be useful for online photo galleries that are positioned up and managed by individual users, including photo blogs. The system used a toy system with two users to demonstrate the principle of the design. It is very efficient than existing system. The system can reduce the privacy leakage by using opensource and Homomorphic Encryption Algorithm. The proposed system features a low computation cost and confidentiality of the training set. Future enhancement can be done by using extended futures of opensource APIs in more efficient privacy training set.

Ashita [4] proposed that an Adaptive Privacy Policy Prediction (A3P) scheme that helps users computerize the privacy policy settings for their uploaded images. The A3P structure provides a wide-ranging structure to suppose privacy preferences based on the in order available for a given user. We also successfully tackled the subject of cold-start, leveraging social circumstance information. Automatic Image Annotation helps to overcome the issue of meta-data information of images being uploaded.

Anna Cinzia Squicciarini [5] focused on an Adaptive Privacy Policy Prediction (A3P) system that helps users automate the privacy policy settings for their uploaded images. The A3P system provides a comprehensive framework to infer privacy preferences based on the information available for a given user. We also effectively tackled the issue of cold-start, leveraging social context information. Our experimental study proves that our A3P is a practical tool that offers significant improvements over current approaches to privacy.

In 2008, Z. Stone, T. Zickler, and T. Darrell [6], portrayed that the delicate and private client traits can be uncovered by the demonstration of tagging pictures on the informal communication site of Facebook. Through Facebook lots of information is being shared which may even be private and exceptionally touchy so a prime concern is given to user privacy. Indeed, even it is been uncovered that even the date and place of birth of a profile can be utilized to anticipate the Social Security Number (SSN) of a Facebook client and extra to considerably more can be uncovered through user friends list. Individuals might be recognized on the photograph through touchy data which might be implanted in the photograph as metadata by going with substantially more data that could be exploited like comments, captions checked areas what's more, photograph labels. Regardless of the possibility that through the photograph labels [2], if the individual is not distinguished, it is conceivable to deduce somebody's character through the combination of face recognition programming and openly accessible information. So it is favored that the clients ought to have the capacity to shroud their labels as opposed to erasing it and along these lines keep a high level of association by monitoring the photographs they have online with the collection proprietor however the photographs shouldn't be connected straightforwardly to their profiles.

In 2008, A. Kapadia, F. Adu-Oppong, C. K. Gardiner, and P. P. Tsang [7] , created protection settings in light of the idea of groups of friends which secures individual data through an online arrangement. The companion's rundowns are naturally created through Social Circles Finder that recognizes the forces of the connection by breaking down the group of friends of the individual which thus helps in classifying of companions for security approach setting. The group of friends of the subject will be distinguished by the application yet won't be uncovered to the subject. The subject's enthusiasm of sharing the data will be considered by investigating the subject and in light of that the bit of individual data will be partaken as visual graphs.

In 2009, J. Bonneau, J. Anderson, and L. Church clarifies security suites [8] which enables clients to effortlessly choose "suites" of security settings that can be made by a specialist utilizing protection programming or can be made through sending out them to the conceptual arrangement or through existing setup UIs. A Privacy suite can be checked by a decent practice, an abnormal state language and persuaded clients which at that point can be then disseminated to the individuals from the social locales through existing circulation channels.

In 2009, JaeYoung Choi', Wesley De Nevel, Yong Man Ro l, and Konstantinos N Plataniotis [9], made utilization of accessible various and conveyed database and furthermore FR motor on OSN to enhance exactness of face comment. This framework used this present reality individual photographs which were accessible on web and the standard MPEG-7VCE-3 informational collection to shape a community oriented FR strategy [9] which enhanced the precision of face comment by considering the comment comes about acquired from singular FR motors. Social relationship among group individuals and social setting in individual photos are utilized to frame FR databases and motors to comment on faces cooperatively as opposed to considering singular FR on which combination strategies are connected to consolidate comes about because of various FR motor and give a solitary outcome. The synergistic framework consequently utilized the face comment strategy to enhance the exactness of the framework which was done through the arrangement of database.

In 2011, Alessandra Mazzia Kristen LeFevre and Eytan Adar [10], clarifies how clients apply security arrangements to their systems. It [10] is an interface and framework that enables the client to perceive its profile in view of various factors, for example, normal sub-groupings of companions that is develop at various phases of granularity. The naturally developed gathering can be consequently perceived and recognized with the assistance of gathering marks. This instrument is superior to anything different devices like Facebook's Audience View and Custom Settings page.

In 2012, Sergej Zerr, Stefan Siersdorfer, Jonathon Hare, Elena Demidova built up a method [11] which empowers protection situated picture scan for consequently distinguishing private pictures. The security strategies are given by mix of literary metadata pictures with assortment of visual components. In this the chose picture features (edges, faces, color histograms) which can help recognize characteristic and man-made articles/scenes should be possible through picture highlights like edges, faces or shading histogram through which the nearness or nonattendance of question can be resolved. The grouping models which are prepared on huge scale dataset are used in which social explanation amusement is utilized to get privacy assignments.

In 2012, Sergej Zerr built up a method [12] which empowers protection situated picture look for consequently distinguishing private pictures. The security approaches are given by blend of printed metadata pictures with assortment of visual components. In this the chose picture highlights (edges, confronts, shading histograms) which can help recognize normal and man-made articles/scenes should be possible through picture highlights like edges, faces or shading histogram through which the nearness or nonattendance of protest can be resolved. It utilizes different order models prepared on a huge scale dataset with security assignments got through a social annotation game.

Sergej Zerr *et al.* [13] proposed a procedure PrivacyAware Image Classification and Search to consequently recognize private pictures, and to empower security situated picture look. It joins printed meta information pictures with assortment of visual elements to give security strategies. In this the chose picture highlights (edges, confronts, shading histograms) which can help segregate amongst normal and man-made articles that can demonstrate the nearness or nonattendance of specific items (SIFT). It utilizes different characterization models prepared on a vast scale dataset with protection assignments acquired through a social annotation game.

Choudhury *et al.* [14] proposed a suggestion structure to associate picture content with groups in online web-based social networking. They portray pictures through three sorts of elements: visual components, client produced content labels, and social connection, from which they suggest the in all probability bunches for a given picture. Correspondingly, a computerized proposal framework for a client's pictures to give reasonable photograph sharing gatherings. Jonathan Anderson *et al.* [2009] proposed Privacy Suites which enables clients to effortlessly pick "suites" of security settings. A security suite can be made by a specialist utilizing protection programming. The security suite is disseminated through circulation channels to the individuals from the social destinations. The downside of a rich programming language is less understandability for end clients. Given an adequately abnormal state language and great coding practice, propelled clients ought to have the capacity to confirm a Privacy Suite. The fundamental objective is straightforwardness, which is basic for persuading compelling clients that it is safe to utilize.

Ching-man Au Yeung *et al.* [15] proposed a get to control framework in view of a decentralized validation convention, clear labels and connected information of interpersonal organizations in the Semantic Web. It enables clients to make expressive arrangements for their photographs put away in at least one photograph sharing locales, and clients can indicate get to control rules in light of open connected information gave by different gatherings.

Danezis *et al.* [16] proposed a machine-learning based way to deal with consequently remove protection settings from the social setting inside which the information is created. It creates protection settings in light of an idea of "Groups of friends" which comprise of bunch of companions. Client's security inclinations for area construct information situated in light of area and time of day.

Fabeah Adu-Oppong *et al.* [17] created idea of groups of friends. It gives an online answer for ensure individual data. The method named Social Circles Finder, which consequently produces the companion's rundown. It is a strategy that examinations the group of friends of a man and distinguishes the power of relationship and in this manner groups of friends acquired an important arrangement of companions for setting security strategies. The application will recognize the groups of friends of the subject however not demonstrate them to the subject. The subject will at that point be posed inquiries concerning their eagerness to share a bit of their own data. In light of the appropriate responses the application finds the visual graph of users.

CONCLUSION

Great amount of data is shared on online social networking. The majority of the time this data consists of images. All this kind of data needs privacy to secure from misuse. However many times applying privacy on data become very complex because of tedious and lengthy process. In this paper, various methods are studied which make privacy setting much easier for user. User's social environment and characteristics, and image's content and its metadata are useful to predict privacy policy for user. Using all this content and above methods privacy recommendation can be easier.

REFERENCES

1. Squicciarini AC, Lin D, Sundareswaran S, Wede J. Privacy policy inference of user-uploaded images on content sharing sites. IEEE transactions on knowledge and data engineering. 2015 Jan 1;27(1):193-206.
2. Klemperer P, Liang Y, Mazurek M, Sleeper M, Ur B, Bauer L, Cranor LF, Gupta N, Reiter M. Tag, you can see it!: Using tags for access control in photo sharing. InProceedings of the SIGCHI Conference on Human Factors in Computing Systems. 2012 May 5 (pp. 377-386). ACM.
3. Xu K, Guo Y, Guo L, Fang Y, Li X. My privacy my decision: Control of photo sharing on online social networks. IEEE Transactions on Dependable and Secure Computing. 2015 Jun 10.
4. Ashita AB. Privacy Policy Inference of User Uploaded Images on Content Sharing Sites with Automatic Image Annotation.
5. Squicciarini AC, Lin D, Sundareswaran S, Wede J. Privacy policy inference of user-uploaded images on content sharing sites. IEEE transactions on knowledge and data engineering. 2015 Jan 1;27(1):193-206.
6. Stone Z, Zickler T, Darrell T. Autotagging facebook: Social network context improves photo annotation. InComputer Vision and Pattern Recognition Workshops, 2008. CVPRW'08. IEEE Computer Society Conference on 2008 Jun 23 (pp. 1-8). IEEE.
7. Adu-Oppong F, Gardiner CK, Kapadia A, Tsang PP. Social circles: Tackling privacy in social networks. InSymposium on Usable Privacy and Security (SOUPS) 2008 Jul 23.
8. Bonneau J, Anderson J, Church L. Privacy suites: shared privacy for social networks. InSOUPS 2009 Jul 15.
9. Choi J, De Neve W, Ro YM, Plataniotis KN. Face annotation for personal photos using collaborative face recognition in online social networks. InDigital Signal Processing, 2009 16th International Conference on 2009 Jul 5 (pp. 1-8). IEEE.
10. Mazzia A, LeFevre K, Adar E. The PViz comprehension tool for social network privacy settings. InProceedings of the Eighth Symposium on Usable Privacy and Security 2012 Jul 11 (p. 13). ACM.
11. Zerr S, Siersdorfer S, Hare J, Demidova E. I Know What You Did Last Summer!: Privacy-Aware Image Classification and Search. InProceedings of the 35th international ACM SIGIR conference on Research and development in information retrieval 2012 Aug 12.
12. Zerr S, Siersdorfer S, Hare J, Demidova E. I Know What You Did Last Summer!: Privacy-Aware Image Classification and Search. InProceedings of the 35th international ACM SIGIR conference on Research and development in information retrieval 2012 Aug 12.
13. Zerr S, Siersdorfer S, Hare J, Demidova E. Privacy-aware image classification and search. InProceedings of the 35th international ACM SIGIR conference on Research and development in information retrieval 2012 Aug 12 (pp. 35-44). ACM.
14. Sundaram H, Xie L, De Choudhury M, Lin YR, Natsev A. Multimedia semantics: Interactions between content and community. Proceedings of the IEEE. 2012 Sep;100(9):2737-58.
15. Yeung CM, Kagal L, Gibbins N, Shadbolt N. Providing Access Control to Online Photo Albums Based on Tags and Linked Data. InAAAI Spring Symposium: Social Semantic Web: Where Web 2.0 Meets Web 3.0 2009 Mar 23 (pp. 9-14).
16. Bonneau J, Anderson J, Danezis G. Prying data out of a social network. InSocial Network Analysis and Mining, 2009. ASONAM'09. International Conference on Advances in 2009 Jul 20 (pp. 249-254). IEEE.
17. Adu-Oppong F, Gardiner CK, Kapadia A, Tsang PP. Social circles: Tackling privacy in social networks. InSymposium on Usable Privacy and Security (SOUPS) 2008 Jul 23.