Scholars Journal of Engineering and Technology (SJET)
Abbreviated Key Title: Sch. J. Eng. Tech.
©Scholars Academic and Scientific Publisher
A Unit of Scholars Academic and Scientific Society, India
www.saspublisher.com

ISSN 2347-9523 (Print)
ISSN 2321-435X (Online)

Sharing of Personal Information Using Online Social Network Securely with Stranger Detection Algorithm

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

Original Research Article

***Corresponding author**
Bhavisha Rajput

Article History
Received: 10.11.2017
Accepted: 07.12.2017
Published: 30.12.2017

DOI:
10.21276/sjet.2017.5.12.2

Abstract: Photo sharing is an alluring component which advances Online Social Networks (OSNs). Sadly, it might release clients' protection in the event that they are permitted to post, remark, and label a photo freely .we endeavor to address this issue and concentrate the situation when a client shares a photo containing people other than himself/herself (named co-photo for short). To avoid conceivable security spillage of a photo, we plan a system to empower every person in a photo know about the posting action and take an interest in the basic leadership on the photo posting. In this paper we address various issues of posting comments and posting using stranger detection algorithm. The algorithm smartly selects the nearby friends in the tree which are supposed to view all your posts and comments hence by restricting remaining friends in personal circle we can gain the privacy.

Keywords: Privacy Policy, Online Social Network, Facebook, Privacy Recommendation, Security, Stranger Detection Algorithm.

INTRODUCTION

With the gigantic ubiquity of sharing and the immense utilization of social systems administration destinations clients unwittingly uncover certain sorts of individual data. Social-systems administration clients might possibly have getting their own data will be released or could master the pernicious assailants and may execute critical security breaks.

The rest decade of 21st century has seen the outrageous advancement of Internet and the development of web administrations which encourage participatory data sharing and coordinated effort. Social Networking Sites (SNSs) have turned into an unfathomable correspondence media to stay in contact past limits. SNSs are a piece of human culture than only a web application. Utilization of SNSs has out separated in practically every field as news offices, of all shapes and sizes organizations, governments, and popular identities and so on to collaborate with each other. With the love of sharing, Facebook has emerged as the most eminence SNSs on the planet where individuals joint for a considerable length of time. With the extravagancy of innovation and administrations sharing of news, photos, individual taste and data with loved ones has prompted straightforwardness. In any case, alongside this client protection ought to likewise be mulled over. An issue identified with protection with facebook clients has been always showing up on universal press either in view of the organizations protection arrangement or due to client's uninformed ness of substance sharing outcomes. As an exploration says the straightforward exposure of date and place of birth of a master le in

Facebook can be utilized to foresee the Social Security Number (SSN) of a subject in the U.S. numerous a times just by basically distributing their companions list; clients may uncover a lot of data. For instance, using expectation calculations it is conceivable to derive private data that was already undisclosed. Now and again touchy data even comes installed in the photo as metadata and may distinguish individuals on the photo by going with more data that could be abused, similar to inscriptions, remarks and photo labels; stamped districts. Regardless of the possibility that the people in a photo are not expressly recognized by photo labels, the blend of openly accessible data and face acknowledgment programming can be utilized to derive someone's character. These sorts of issues are characterized as inadvertent blow-back: clients unexpectedly put their own particular security or their companion's security in danger when performing occasions on SNSs, for example, Facebook.

Before, there was a buzz in regards to the protection settings of Facebook as it was extremely muddled however later they have disentangled it for better understanding and simple access to average folks. Because of absence of learning and comprehension of security highlights of Facebook, individuals make many oversights. Another essential thing which ought to be controlled is the accessibility of the individual data which ought to be kept from spillage as it might uncover individual data of a person as recordings, pictures or any information.

As the ubiquity of social networks keeps on developing, concerns encompassing sharing data online compound. Clients routinely transfer individual stories, photos, recordings, and arrangements of companions uncovering private points of interest to the general population. To secure client information, protection controls have turned into a focal highlight of social systems administration locales yet it stays up to clients to embrace these highlights. Protection limitations frame a range amongst open and private data.

On the general population end, clients can permit each Facebook part to see their own substance. On the private end, clients can confine access to a particular arrangement of put stock in clients. Facebook utilizes fellowship to recognize trusted and untrusted parties. Clients can permit companions, companions of companions, or everybody to get to their profile information, contingent upon their own necessities for security. 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 *et al.* [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.

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 open source and Holomorphic 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 open source 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.

METHODOLOGY

In this section we will discuss about the proposed methodology. The system architecture is shown in fig. 1.

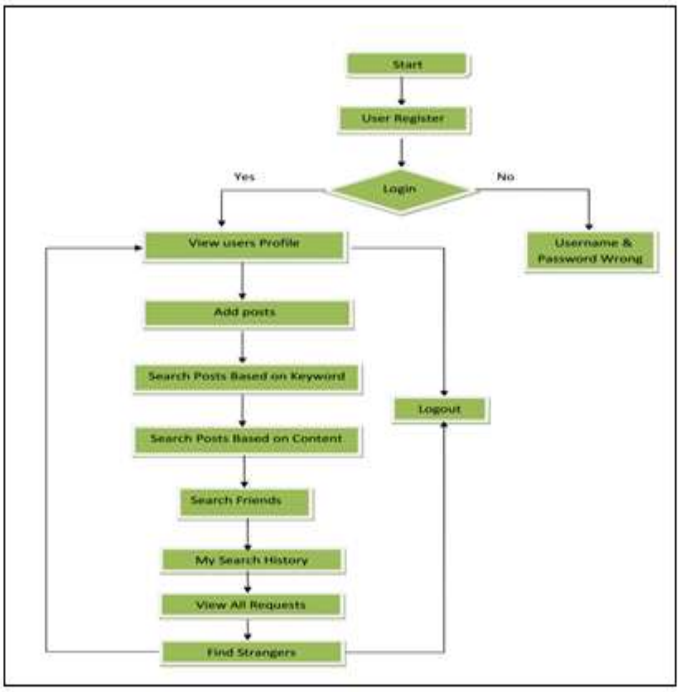


Fig-1: Shows System Architecture

- **User Registration**

The user first register in the proposed framework which is made exactly as facebook.

- **Login**

After registration user can login into account and can update details.

- **Add Posts**

The user can share personal information with other friends. The user has several options to select while posting the posts.

- **Selection of Friends**

The user can select friends to whom to show the posts. This way user can restrict the users.

- **Selection of Cloud Storage**

This way user can just uplaod the images in the OSN cloud so that it can be retrived later. Posting of post can be also done through which all the user can able to see the content.

- **Search Posts**

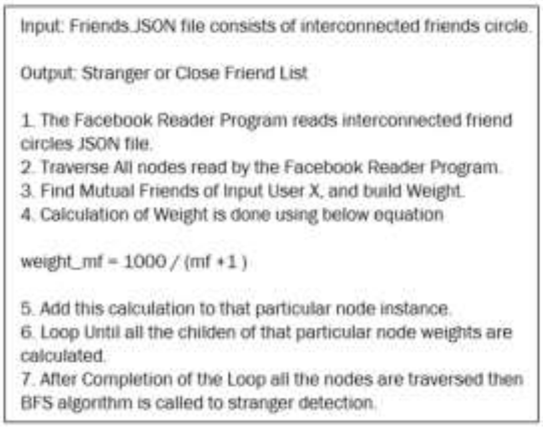
The User can search posts based on two algorithm.

- Content based text retrival.
- Content based keyword retrival.

In both the case content from the users are retrived.

- **Stranger Detction**

The proposed technique for finding strangers in user account. It generally constuct a tree through which the stranger from fartherst nodes can be detected.The algorithm is presented in fig 2.



Input: Friends JSON file consists of interconnected friends circle.

Output: Stranger or Close Friend List

1. The Facebook Reader Program reads interconnected friend circles JSON file.
2. Traverse All nodes read by the Facebook Reader Program.
3. Find Mutual Friends of Input User X, and build Weight.
4. Calculation of Weight is done using below equation

weight_mf = 1000 / (mf +1)

5. Add this calculation to that particular node instance.
6. Loop Until all the childen of that particular node weights are calculated.
7. After Completion of the Loop all the nodes are traversed then BFS algorithm is called to stranger detection.

Fig-2: Shows the Stranger detection algorithm

The dectection algorithm starts from taking input the JSON file. For user A, all the friends are connected via a node.

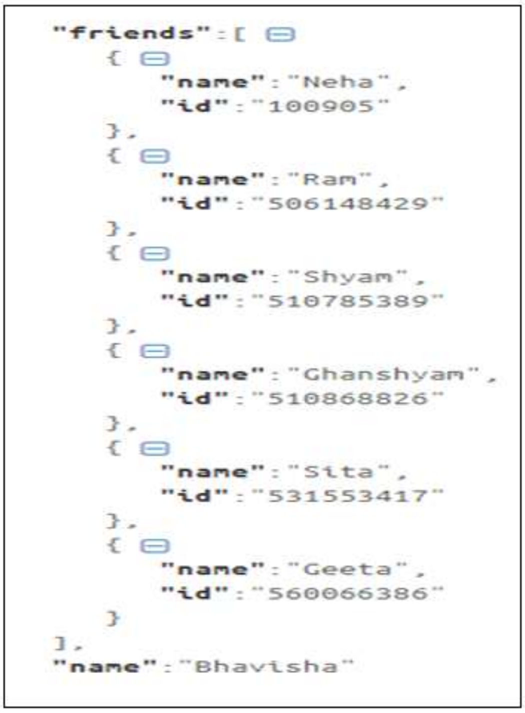
For each node the below formula is evaluated.

$$weight_{mf} = \frac{1000}{mf + 1}$$

Where the aims of the equation is to fnd the closeness of each nodes from user A. The mf represents the mutual friend list.

RESULTS

The dataset are generated randomly to show the proof of concept. The dataset generated as shown in fig. 3.



```
"friends":[
    {
        "name":"Neha",
        "id":"100905"
    },
    {
        "name":"Ram",
        "id":"506148429"
    },
    {
        "name":"Shyam",
        "id":"510785389"
    },
    {
        "name":"Ghanshyam",
        "id":"510868826"
    },
    {
        "name":"Sita",
        "id":"531553417"
    },
    {
        "name":"Geeta",
        "id":"560066386"
    }
],
"name":"Bhavisha"
```

Fig-3: Shows the user Bhavisha Friend's JSON File

When stranger detection algorithm runs, the following results are obtained for each node which clearly tells about the stranger of the user. Table I shows the distance between two friends.

Table- 1: Shows closeness of different users, considering "bhavisha" as a base user

SNO	User Name	Closeness	Friend
1	Alice	0	NO
2	Bob	0	NO
3	Geeta	166	YES
4	Ghanshaym	142	YES
5	Neha	142	YES
6	Ram	142	YES
7	Shyam	142	YES
8	Sita	166	YES

From table I, we can conclude that since alice and bob are not in the friend list of Bhavisha, they are stanger. User geeta and sita are friends of Bhavisha but they are too far from bhavisha in the decision tree. So they are not able to view the contents of bhavisha's posts.

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, we proposed a novel mechanism for finding stranger from user friend list. Also, we proposed a mechanism for sharing information to only those who are close enough to be shared information.

REFERENCES

1. Squicciarini AC. "Privacy Policy Inference of User Uploaded Images on Content Sharing Sites. IEEE Transactions on Knowledge and Data Engineering. 27(1), January 2015.
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. 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.
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).