ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

# Securing Photo by a Secured Decision to Attain High Privacy in OSN

Shelma Joseph M[1], Niyas N[2]

M. Tech, Department of Computer Science, KMCT College of Engineering, Kozhikode, Kerala, India

Assistant Professor, Department of Computer Science, KMCT College of Engineering, Kozhikode, Kerala, India

**ABSTRACT**: An online social media is most common forum in today's world. An OSN is used for debates, sharing news, sharing views, pictures, videos and lot more. Every OSN user has lot of concern about their own privacy. Any user who is an active participant of any online social media network has a very important part of educating themselves and their near ones about the way security and privacy settings are configured. Though OSN is there for lot of things like but it is also a hub for hackers and scammers and makes things worse for others. Every user's security is his own rights and its completely based on his/her decision. This paper discusses about the process of how we can attain high privacy with a secured decision we make and how it can be further avoided in involving us into the loop.

**KEYWORDS**: OSN, Face Detection,Face Recognition, Secured Computing, Photo sharing

## I. INTRODUCTION

Online social network has become a very important part of day to day life and has completely changed the way we share information, the way we have social communication and the way we talk to each other. In today's world most of the people just don't think about anything before posting anything on a social media network. Once we post a photo or a video that makes a permanent record in the internet which can be used for lot of unwanted things that we would have never imagined or expected. This can be explained with an example too. Consider X is a celebrity, Y posts a photo with X which will reveal their friendship to the whole world and create issues for X.The situation becomes even worse when photo tagging and sharing comes into the picture.

To get more people involved in the activities of a social networking site. Online social networks like face book encourages users to post photos as well as tag those people who are there in this photo and other friends .The photos that are shared doesn't have any rules too. So coming to the main concern, when we share and tag the photo what if one person in the photo or more than one person in the photo are not willing to share their photo. What if the person think he also should have rights while his photo is shared .To address this issue we need to have a clear study about the privacy issues in and over OSN .Privacy is never moving away from from a social network. As Altman says about privacy regulation theory [1][2] "privacy is a dynamic and dialectic boundary regulation process where privacy is not static but "a way a person becomes selective in control of access to the self or to ones group". Dialectic means closeness and openness of a person to others and the word "dynamic" refers to desired level of privacy keeps changing with time respect to the environment.

Actually during the process of regulating the privacy, we try to match the achieved privacy level to the one we desire. At the starting level of privacy, we can experience the confidence we desire when we don't want to show and when we want to enjoy the attention we desired that we wish toexhibit toeverybody. The problem arises when we don't want to exhibit to everybody but it happens through other resources and we don't have control over it. As per Kaihe Xu, Yuanxiong Guo, Yuguang Fang,Linke Guo and Xiaolin Li, says about how we can control photo sharing on online social network by the decision we make[4] gives a solution to the above mentioned problem. But the question asked every time to the user when the photo is posted is a disturbing .So this paper proposes how this question system can be eradicated and still maintain the high privacy. Concluding the statement, if the actual privacy level is more than the desire level then we will feel left alone or isolated; on the other side if the actual privacy level is smaller than the desired level we will feel vulnerable or over exposed.

## II. RELATED WORK

In [1] the authors describe an approach how protection can be enabled for shared data that is associated with multiple users in OSN.The authors have formulated an access control model to capture the essence of multipart authorization requirements and also about multiparty policy specification scheme and enforcement scheme. In [2] the author discuses about the review of different privacy risks and security risks, which is a big, threaten to OSN users in general especiallychildren. Adding to that the authors present an overview of the solution that is already present for the protection, security and privacy of users .The authors also discuss about the simple implementations for OSN users which will improve the security and privacy concerns. In [3] the authors highlights how influence of the interpolation and the similarity measurementmethods works on the efficiency of the fractional Eigen faces algorithm with the use of ORL,YALE & UMIST database. In[4] the authors describes a face detection framework which is capable of processing images extremely fast while achieving high detection rates. There are three key contributions are, introduction of a new image representation called the “Integral Image” that allows the features used by our detector to be computed fast. Next is a simple and efficient classifier that is built using the AdaBoost learning algorithm. This method selects a small number of critical visual features from a very large set of potential features. The last contribution is a method for combining classifiers in a “cascade” which allows background regions of the image that will be quickly discarded while spending more computation on promising face-like regions. In [5] the authors propose a diversified one-against-one method helps to find the best classification method for each pair when applying one –against –one approach to multi classification problems. In[6] the authors have discussed about faster face detection using skin colour and AdaBoost.In [7] the authors describe how to prevent privacy leakage of a photo by designing a mechanism by enabling each individual in the photo to be aware of the posting activity and participatein the decision making of photo sharing.

## III. PROPOSED ALGORITHM

### A. *Privacy Levels*

**Posting Photos-Without Privacy**

When we consider posting the photos in OSN in the initial days, we didn’t have any option to select the privacy .All photos were visible to every on and anybody could access our photos. While resulted in lot of misuse of photos. This misuse of photo lead to lot of problems. There was always a fear of posting our own photos. This lead to people posting fake pictures such as dolls, flowers or any other relevant photos.

**Posting Photos-Privacy Options**

Users in an OSN share a lot of information like photos, their views, videos, long messages but the importance of privacy implications of doing so has yet to come .We understood from the previous topic how bad it is when we don’t have any privacy in our online social network. There are three factors that discuss on privacy, they are1.A online social network user reveals too much information;2. A social networking site doesn’t take too many steps to protect user privacy; 3.There is so many people outside waiting to get user information to make use of it in a wrong manner. That’s when a online social networking site like face book came with flexibility in privacy option, which was considered to be a good deal.The user settings option of privacy in their own social networking page allows a user to decide and specify the people to whom they can be visible during searches, which will allow them to see their profile, to get their contact details and their photos. Adding to that privacy option, there is also a block option to block few users whom we feel are unnecessary. As per the usage agreement, a specific OSN user can request OSN not to share any of their information with any third parties.

**Posting Photos –Tagging Options**

What is tagging? It is a method of pointing your friends or anyone else the photos that you post on a online social network This tagging creates a link that anybody can follow and get information about who all there in that photo. What can a tag do? It add people in the photo, give them information about that photo, help them follow the other posts about that photo and help them receive notifications ,involve people in sharing information about that photo. You can tag any photo and add details to it. If you are not interested in any tagging, we can untag that with following options

**a. Tag Removal**. It won be on your wall but on the friends wall who posted it.

b. **Send a message-To the owner:** Mention the reason and send a message to the owner

c. T**o Face book -Send a report**. : Report its abusive and sooner it will be removed

d.**Block-The owner of the post**: the person who was blocked cannot see your post

**Posting Photos –With Security Questions**

On most current OSN , ,a user is not in a position to decide what appears outside the page. In [3], Thomas, Grier and Nicol examine how joint privacy is less and if we don't control we can inadvertently reveal sensitive information about a user. To remove this threat, they suggest OSN's privacy model to be adapted to achieve every body's privacy. Specifically, there should be a mutually acceptable privacy policy determining which information should be posted and shared For example, people showing up together on a photo can be posted on the wall, but if there is one person who is not willing the to post but has no other option other than un tagging himself. The problem doesn't stop there, he/she can hide the post only from their page but the photo will appear on other's wall.

Posting photos with security questions sends a same time to all the people found on the photo, only when all accept to post the photo the photo comes on the wall. This method will minimize the number of un wanted photos being uploaded.But the user will be nagged too many times with same questions for which we come up with the proposed method.

B. ***Description of the Proposed Algorithm:***

The aim of the proposed method is to eradicate this problem we develop in automatic analysis ,where the system will ask the user every time when the person says " No " when the security question is asked .This analysis will have few questions. Based on the answer the we predict the next time we post a photo and decide whether the photo has to be posted or not. This prediction is done using k means algorithm by clustering each individual to different clusters that we have created. This approach will reduce the waiting time in the future and avoid unnecessary same time questions send to all users in the photo. To attain this approach we have do the following

Step 1: **Training**

Once a profile is created, with which a person id is also created .The user uploads a profile photo .This profile photo is used for creating a data set of the user. When the profile is created the user will be allowed to put a photo with single user in it and will be asked a question whether it is him in the photo .If the user says it is him, that particular photo will be stored as his face id(i.e. Corresponding to his person id) in the date set.

Step2: P**hoto Uploading**

A group photo is uploaded with different users in it.

Step 3: **Face Detection**

The face detection in the group photo is done using tracking js library which bring a different techniques and computer vision into the browser environment. By using HTML 5 we can detect face in real time

Step 4: **Face Recognition:**

Face recognition is done using Microsoft cognitive service face API which is a cloud-based service that has most advanced face algorithms. Face API has two main functions: face detection with attributes and face recognition. Face rectangle (left, top, width and height) indicating the face location in the image is returned along with each detected face. Optionally, face detection extracts a series of face related attributes such as pose, gender, age, head pose, facial hair and glasses. Face recognition is widely used in many scenarios including security, natural user interface, image content analysis and management, mobile apps, and robotics. Four face recognition functions are provided: face verification, finding similar faces, face grouping, and person identification. This API can be further used for face verification, finding similar faces, face grouping and face identification.

**How it works?**

Once a person uploads a group photo, the face will be detected and will be compared with the different face ids in the data set that we have trained using the profile pictures. Using Person Id the security question can be send to the user.

Step 5: **Security Questions**

After the face is detected and recognized the user is asked with few security questions based on which the user is classified. The security questions are in the following

John wants to post a photo with you?

YES NO

If the user selects “yes”, the photo gets posted and if the user selects “No” he will be asked the following questions

1. Inform me everytime □

2. Post’s content is not good for me □

3. This is not posted by my friend □

4. I am not happy with this post’s occassion □

5. Some other personal reason

Step 5: Automatic Analysis

The user will be prompted with these questions when he selects the option “No” .Based on the answer he will be classified into one of the classifierusing the concept of K means algorithm. He will classify into one of the classifier based on his answer for three consecutive questions.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

1. Open Person
2. Deep
3. Friend
4. Strict
5. Content
6. Other

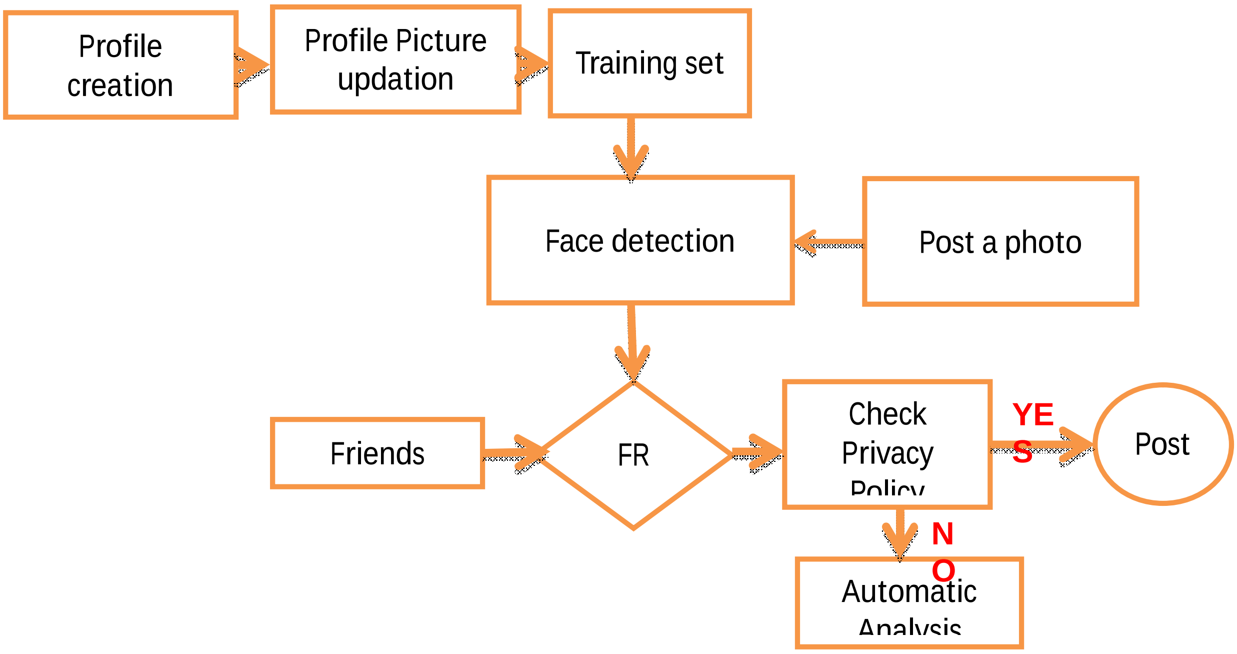

Fig 1: System Structure

## IV. Pseudo code

```
Step 1: Generate Face ID and Person ID
Step 2: Compare the face with the Face ID in the database, when it matches look for the corresponding Person ID
Step 3: Send Message "Whether you want to post a picture"
Step 4: Check the condition
if (answer== yes)
            Post the photo
        else
            Ask Security Questions

Step 5: Classify according to the answerinto any of the classifier.
Step 6:  Repeat the process for three times
Step 7: END
```

## V.SIMULATION RESULTS

*A. Evaluation*

The evaluation of this system is done with one criteria: Security with different scenarios.

| **Features** | **Existing Method** | **Proposed Method** |
|---|---|---|
| Privacy | Less Privacy | More Privacy |
| Security | Less security | More security |
| Photo availability in OSN | yes | Based on user's decision |
| Repetition of security questions | yes | No |
| Stranger Recognition | 10% | No Stranger recognition |

Table 1: Comparison of Existing Method and Proposed Method

*B.IMPLEMENTATION*

The system is implemented as a online social networking web site and a android application.

## VI. CONCLUSION AND FUTURE WORK

This system completely designed for the benefit of a user in terms of their security and privacy .The user in the system is benefited out of it. But a stranger recognition in the group photo and sending a security question is a concept that has thought through as future work.

## REFERENCES

1. Pitta Venkatesh and Mr. Reddi Prasad,"Multiparty Access Control for Online Social Networks:Model and Mechanism,International Journal of Academic Research,ISSN:2348-7666,Vol 2Issue-1(4),January-March 2015.
2. Michael Fire, Member, IEEE, Roy Goldschmidt, and Yuval Elovici, Member, IEEE,"Online Socal Network Threats and solution", IEEE COMMUNICATION SURVEYS & TUTORIALS, VOL. 16, NO. 4, FOURTH QUARTER 2015
3. Ahmed Ghorbel, Member, IEEE, Imen Tajouri, Member, IEEE, Walid Elaydi, Member, IEEE, Nouri MasmoudiMember, IEEE," The effect of the similarity measures and the interpolation techniques on Fractional Eigenfaces algorithm", 978-1-4799-9907-1/15/$31.00 ©2015 IEEE.
4. Paul Viola , Microsoft Research, One Microsoft Way, Redmond, WA 98052, USA,"Robust Real time face Detection" International Journal of Computer Vision 57(2), 137–154, 2004
5. Seokho Kang , SungzoonCho , PilsungKang," Constructing amulti-classclassifier usingone-against-oneapproach with differentbinaryclassifiers" www.elsevier.com/locate/neucom
6. Saiping Ji, Xiaobo Lu*, Qianzhou Xu ," A Fast Face Detection Method Combining Skin Color
7. Feature and AdaBoost " ,National Natural Science Foundation of China (No. 61374194), the National Natural Science Foundation of China (No. 61403081), and the Natural Science Foundation of Jiangsu Province (No. BK20140638).
8. Kaihe Xu, Student Member, IEEE, Yuanxiong Guo, Member, IEEE, Linke Guo, Member, IEEE, Yuguang Fang, Fellow, IEEE,Xiaolin Li, Member,IEEE.MyPrivacy MyDecision Control of photo sharing on OSN 10.1109/TDSC.2015.2443795 IEEE Transaction
9. Altman. Privacy regulation: Culturally universal or culturally specific? Journal of Social Issues, 33(3):66–84, 1977
10. L. Palen. Unpacking privacy for a networked world. pages 129 to 136. Press, 2003.
11. K. Thomas, C. Grier, and D. M. Nicol. Unfriendly: Multi-party privacy risks in social networks. In M. J. Atallah and N. J. Hopper, editors, Privacy Enhancing Technologies, volume 6205 of Lecture Notes in Computer Science, pages 236–252. Springer, 2010.
12. J. Y. Choi, W. De Neve, K. Plataniotis, and Y.-M. Ro. Collaborative face recognition for improved face annotation in personal photocollections shared on online social networks. Multimedia, IEEE Transactions on, 13(1):14–28, 2011.
13. H. Yu, X. Jiang, and J. Vaidya. Privacy-preserving svm using nonlinear kernels on horizontally partitioned data. In Proceedingsof the 2006 ACM symposium on Applied computing, SAC '06, pages 603–610, New York, NY, USA, 2006. ACM.
14. Z. Stone, T. Zickler, and T. Darrell. Toward large-scale face recognition using social network context. Proceedings of the IEEE,98(8):1408–1415.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

*Website: www.ijircce.com*

Vol. 5, Issue 4, April 2017

## BIOGRAPHY

**Shelma Joseph M** perused her B.tech inInformation Technology from Karunya University and currently perusing M tech in KMCT college of Engineering. Worked in IT for two years and as a lecturer for 2 years. Her Research includes image processing, secured computing and face recognition

**Niyas N** received his B.Tech. degree inComputer Science and engineering from Cochin University for Science and Technology and MTech degree in Computer Science from University of Calicut.He has a broad span of experience in IT industry as well as Teaching. He is currently working as Assistant Professor in KMCT College of Engineering, Kozhikode. His research interest has a wide range including Image Processing and Supervised Machine Learning .

DOI: 10.15680/IJIRCCE.2017. 0504218