ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 1, January 2017

A Survey on Photo Sharing and Privacy Management Over Online Social Media

Monica Bunge[1], Archana Kalbhor[2], Komal Kardile[3], Sonal Zagade[4]

U.G. Student, Department of Information Technology Engineering, JSCOE, PUNE, Maharashtra, India[1]

U.G. Student, Department of Information Technology Engineering, JSCOE, PUNE, Maharashtra, India[2]

U.G. Student, Department of Information Technology Engineering, JSCOE, PUNE, Maharashtra, India[3]

U.G. Student, Department of Information Technology Engineering, JSCOE, PUNE, Maharashtra, India[4]

ABSTRACT: In web social media the web users may, however, face the risk of leaking their personal information Photo sharing is an attractive feature which popularizes on social media. Unfortunately it leaks users privacy if they allowed to post, comment, tag a photo, blurring photo and downloading photo freely. We attempt to address this issue and study the scenario when a group shares a photo. To prevent possible privacy leakage of a photo, we design a mechanism to enable each individual in a photo be aware of the posting activity and participate in the decision making on the photo posting by using SVM(Support Vector Machine).For this purpose, we need an efficient Face Recognition(FR) system that can recognize everyone in the photo. We provide facility anyone should not download our photo and chatting is in the encrypted format. We provide facility anyone should not download our photo and chatting is in the encrypted format.

KEYWORDS: Social media, photo privacy, Machine learning, secure multi-party computation.

I. INTRODUCTION

Social sites have become important part of our daily life. Online social networks (OSNs) such as face book, Google are inherently designed to make able people to part personal and public information and make social connections with friends, co-workers, persons having like position, family, and even with strangers [1]. Social media used to connect the people together by grouping themself. They can share their information, text, images, audio, video etc. Images are important part of our life, because images are used to connect the people together in social media [2]. Most of the time youngsters are used to share their personal information of images, through social media. Due to lack of awareness among user and presence of less privacy tools, user personal information, pictures or images, is at risk [4]. They can be used by strangers, recruiters and even the public at large, in any way which they want. Most of the times user is against to get tagged or being exposed without his permits. Is it misbehaviour if we share picture without taking permission from all the people involved in picture? To answer this we need to explain the privacy and security issues over the social media [1]. We provide additional operation to user. User will have option to accept or reject the tag.

II. RELATED WORK

Social media are integral part of our daily life. Websites such as Facebook, Google+ have millions of user across the globe. Online social media are mainly used to share their interest, text and pictures. While sharing such images, privacy has become an important issue [3][4]. Currently there is no restriction with sharing photos or images with tagging features. It allows user to post photos and tag their friends in order to get more people involved. But what if the people, who are tagged, are not allowing sharing their photos or images? It is privacy violating to share this photo without permission of tagged person. Should the tagged people have same control over the photos? To answer this question "photo sharing and privacy management over online social media" we provides facility to tag friends. Among these

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 1, January 2017

friends, who added photo to their timeline can only visible in that photo. The friends who are not willing to share their photos, gets blurred to avoid privacy issue.

III.METHODOLOGY

A. FACE RECOGNITION SYSTEM

We propose a privacy-reserving distributed collaborative training system as our FR engine. In our system, we ask each of our users to establish a private photo set of their own [1] [7]. We use these private photos to build personal FR engines based on the special social context and promise that during FR training, only the discriminating rules are revealed but nothing else with the training data distributed among users, this problem could be formulated as a typical secure multi-party computation problem [6]. Intuitively, we may apply cryptographic technique to protect the own photos, but the computational and communication cost may pose a serious problem for a large OSN.

Step 1: Classifier initialization
i: LoadBodyClassifier = clbody
ii:LoadF aceClassifier = clface
Step 2: Image initialization
i:GetInputimage = Iin
ii:Igray = convert(Iin; grayscale)
iii:Igray = histequalise(Igray)
Step 3:Body Detection
Vectdet - body = detect - multiscale (Igray; clface)
Step 4: Face detection inside the bodies
i:Vecdet - face = detect – multiscale(Igray; clface)
Step 5: Body face check and amp; data storing
For all(det - body)
If(det - face > det - body)
Body[i] = det – body
Face[i] = det - face next i
Step 6: Target person selection
If(selection - key == pressed)
Input(K) target - id = k
Else goto (step3)

B. ADVANCE ENCRYPTION STANDARD ALGORITHM

Advance encryption is a form of encryption that allows computations to be carried out on cipher text, thus generating an encrypted result which, when decrypted, matches the result of operations performed on the plaintext [8]. Advance encryption would allow the chaining together of different services without exposing the data to each of those services.

Step 1. Do the following one-time process
a. Multiply the 16-byte key to get the actual Key block to be used
b. Do one time initialization of the 16-byte plain text block
c. XOR the state with key

Step 2.Initialize the state array with the block data (plaintext)
a. Apply S-box to each of the plain text byte
b. Rotate row k of the plain text block (i.e. state) by k bytes
c. Perform a mix column operation
d. XOR the state with key block.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 1, January 2017

IV. EXPERIMENTAL RESULTS

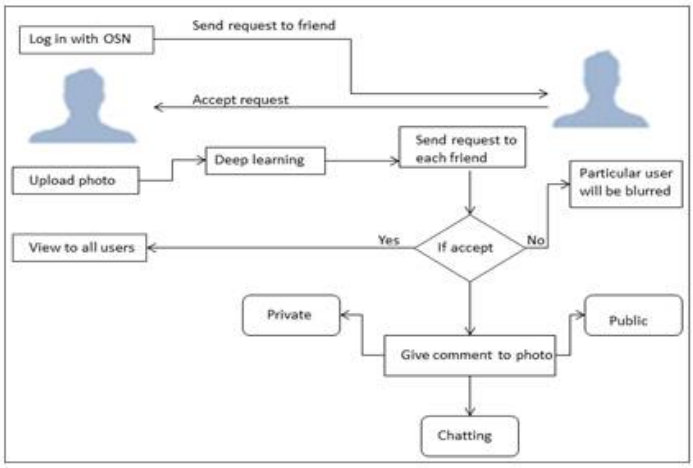

Fig (1): System Architecture

In fig (a), the system covers different domains one is the machine learning followed by deep learning. Deep learning is used for classify the image whether it is a human image or not. In deep learning we use five models in the form of artificial neutral network. At the bottom three models will be used. In this we identify whether image content eyes, nose, lips present or not. At the middle level two models will be used. In this we identify whether image content two eyes and one nose. At top most level we get classification for the image. Fig (a) shows the graphical user interface. A log in/out button could be used for log in/out with Facebook. After logging in, a greeting message and the profile picture will be shown. Our prototype works in three modes: a setup mode, a sleeping mode and a working mode.

Upload Photo: Uploading means data or photo sent from your device to the internet. In our system user upload photo and then send request to each person in group photo. If accept that request then view that uploaded photo otherwise blurring image displayed to each user.

Send Request: the user can find his/her friend based on preferences set in profile and then send request to his friend. In this module after uploaded group photo then user send request to each person who is present in that photo.

Accept request: In this module who is present in group photo want to share his/her photo on social media then he/she accept the request otherwise reject the request.

Chatting: In this module chatting is displayed to all users in encrypted format. We use AES algorithm for chatting, in which plaintext get converted into cipher text which is unreadable format [8]. Chatting is text based communication that is real time.

Comments: comment is a give compliment to other peoples. Sometimes comment may be good or bad. If comment is in bad form then it affect person will get hurt. In our system two type of comments. one of them is private and second is public. In Private, if comments are bad and person doesn't want to share this comment to everyone then he reject request then it is view to only particular user. Suppose comment is good form then person accept request for that comment and it will get displayed to everyone.

Blurring Image: In this module, blurring is method in which we make image or photo invisible. For example, In below image there are two user, user A and user B. If user B upload the photo on social media but user A not willing to share his photo on social media. Therefore we provide more customized option to the user. We will be use Face Recognition

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 1, January 2017

System for blurring the particular person in the photo. User will have accept or reject request to share photo on social media.


(b) Before (c)After

(d)

Deep learning: It is concept of machine learning which is used for detecting whether an image has human face or not.in machine learning approaches huge amount of labeled or unlabeled images are given as input in term of pixel wise value.

V. CONCLUSION

Photo sharing and chatting is one of the most popular features in online social media such as Facebook. To prevent the privacy leakage, we proposed to enable individuals in a photo to give the permissions before posting a group photo and chatting is in encrypted format. We designed a privacy preserving FR system to identify individuals in a group photo. We expect that our proposed scheme be very useful in protecting users privacy in photo sharing and chatting over online social media.

REFERENCES

[1] Kaihe Xu,Yuanxiong Guo,Linke Guo,Yuguang Fang,Xiaolin Li."My Privacy My Decision: Control of Photo Sharing on Online Social Networks" IEEE 1545-5971 (c) 2015
[2] I. Altman. "Privacy regulation: Culturally universal or culturally specific? Journal of Social Issues", 33(3):6684, 1977
[3] Ramesh Bandaru and Rao S Basavala,"Information Leakage through Social Network-ing Websites leads to Lack of Privacy and Identity Theft Security Issues",2013
[4] Rijavan A. Shaikh , Ms. Rachana Kamble "A Survey Filtering Unwanted Post from OSN User Wall using Automatic Blacklist Generation", IJMTER-2015
[5] M. Muthubrindha, Dr. A. Valarmathi "Privacy Based Image and Comment Sharing on Online Social Networks Based on Short Text Classification",April 2016
[6] K. Choi, H. Byun, and K.-A. Toh. "A collaborative face recognition framework on a social network platform. In Automatic Face Gesture Recognition", 2008. FG '08. 8th IEEE International Conference on, pages 16, 2008
[7] J. Y. Choi, W. De Neve, K. Plataniotis, and Y.-M. Ro. "Collaborative face recognition for improved face annotation in personal photo collections shared on online social networks. Multimedia", IEEE Transactions on, 131):1428, 2011
[8] M.Pitchaiah, Philemon Daniel, Praveen" Implementation of Advanced Encryption Standard Algorithm" International Journal of Scientific & Engineering Research Volume 3, Issue 3, March -2012 ISSN 2229-5518 IJSER © 2012