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 5, May 2017

Fake Account Detection and Privacy Policy Inference based on content-based classification of User-Uploaded Images on Content Sharing Sites

Anant Mandre[1] , Prof. Sonali Patil[2]

M.E Student, Dept. of Computer, JSPM's BSIOTR, Pune, India [1]

Asst. Professor, Department of Computer, JSPM's BSIOTR, Pune, India [2]

ABSTRACT: In this era, there is an increasing wave of image sharing & fake accounts via social media sites. Though image sharing is the need of users or most favorite activity of users on social networking sites, ensuring the privacy of images is becoming critical. When the peoples are communicating with each other, they are sharing their professional, personal & political data with each other. The malicious entities attracts towards such information & fake people trying to exploit the vulnerabilities on the social networking sites. There have been many recent reported occurrences where users unintentionally shared personal data. By looking at the increasing rate of such incidents there is a high need for tools to provide privacy to the content that user share on social media sites. For this need, we tend to propose a system which recommends Privacy Policies for user-uploaded images on social media sites and easily detect fake account. We tend to examine the role of social context, image content, and Metadata as potential indicators of user's privacy preferences. We tend to propose a two-level framework that in keeping With the users accessible history determines the most efficient privacy policy for the user's pictures being uploaded. We also propose Decision Voting system to recommend the Privacy Policies at the individual level for the further security of images, Image Encryption is proposed. This ensures Conflict Resolution while assigning the policies at the individual level.

KEYWORDS: Fake account detection, Social media, Content sharing sites, Privacy, Meta data, Content-Based Classification system, Fake user detection algorithm.

I. INTRODUCTION

On-line Social Networks (OSNs) are increasingly becoming the medium for people to keep in touch, share information about their daily activities, travels, photos, and political upraising. Depending on the nature of the social connections, features and the structure of the OSNs may vary significantly from each other. For example, a typical professional social network (as LinkedIn) may not contain family or personal friends as part of the network, while a network based on hobbies may not contain members from the professional social network.

Hundreds of millions of people on Social Networking can swap their content through media, text like audio, video image etc. It will provides a content sharing mechanism and connects people across the global. The social media users can define a personal profile and change it as they wish. Through this social media, users may engage with each other for different purposes like knowledge sharing, business and leisure. People use social networking sites to get in touch with further people, and create and contribute content that includes personal information, videos and images. The service providers have admission to the content presented by their users and have the right to collect data and share them to unauthorized users. End users are nevertheless often not aware of the nature or size of the spectators accessing their data and the sense of understanding created by organism among digital users and friends. The success of the Social Network based on the number of users it attracts, and cheering users to add more users to their circle and to share data with other users in the social network. So the information will go beyond the global world. In general, similar images often incur similar privacy preferences, especially when people look in the images.

Take example, one may upload many photos of his children's and specify that only his family members are allow to see that images. He may upload some other photos of that places which he took as a interest and for these images, he may set secrecy preference allowing anyone and any other to view and comment on that photos. Analyzing visual

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 5, May 2017

content may not be sufficient to capture users privacy preferences. Other data about that data and Tags are indicates of the social network context of the photos, that including where as well as why it was taken and also provides the detail description of images, complementing the information obtained from visual content analysis.

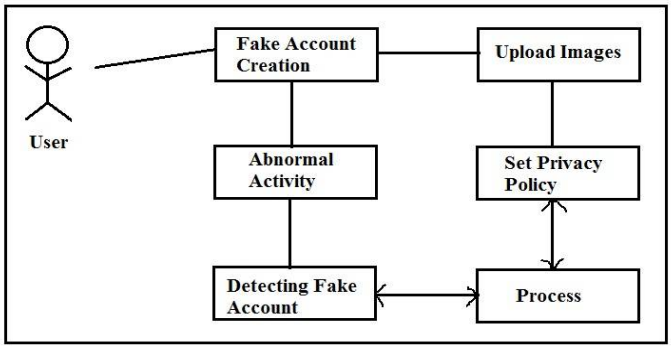
II. RELATED WORK

Morteza Yousefi Kharaji and Fatemeh Salehi Rizi in 2014, In this paper at a recent time, a new kind of attack which is named Identity Clone Attack is detected on online social networks that makes fake profiles of specific users. The basic goals of the enemy in this attack are gaining victims friends private information by forging real user profile, and growing trust among mutual friends to do more defrauding in the future.Two kinds of these attacks areal ready defined: first is Single-Site Profile Cloning, and the other one is Cross Site Profile Cloning. The first attack gives enemy forges the real user profile in the same social network as well as use this cloned profile to send friend request to users friends. The unaware user can be think that this request is came from a familiar user hence she/he will confirm that request and his/her private and personal information will be accessible for enemy. [1].

Mauro Conti, Radha Poovendran and Marco Secchiero in 2012, gives the a possible approach to mitigate the threat of the Fake Profile Attack, where an adversary tries to impersonate a victim on an On-line Social Network where the victim has no prior profile in place.On-line Social Networks (OSNs) are increasingly influencing the way people communicate with each other and share personal, professional and political information. Like the cyberspace in Internet, the OSNs are attracting the interest of the malicious entities that are trying to exploit the vulnerabilities and weaknesses of the OSNs. Increasing reports of the security and privacy threats in the OSNs is attracting security researchers trying to detect and mitigate threats to individual users. With many OSNs having tens or hundreds of million users collectively generating billions of personal data content that can be exploited, detecting and preventing attacks on individual user privacy is a major challenge. [2]. M. Mazurek, M. Sleeper, B. Ur, and M. Reiter L. Bauer, N. Gupta and Klemperer in 2012 find the a) users tagging with access control in mind develop the correspondent strategies which lead the significantly more accurate rules than those associated with organizational tags alone,b) participants can be actively engage and understand with the concept of the tag based access control,c) tags created for the organizational purposes may repurposed to create an efficiently and reasonably accurate access control rules. [3].

III. PROPOSED ALGORITHM

A. *Proposed System Architecture :*



Consider a photo of a student's 2016 graduation ceremony, for example. It could be shared within a Google+ circle or Flickr group, but may unnecessarily expose the student's family members and other friends. Sharing images within online content sharing sites, therefore, may quickly lead to unwanted disclosure and privacy violations. Further, the persistent nature of online media makes it possible for other users to collect rich aggregated information about the owner of the published content and the subjects in the published content. The aggregated information can result in unexpected exposure of one's social environment and lead to abuse of one's personal information.

Our work is related to some existing recommendation systems which employ machine learning techniques. Chen et al.proposed a system named Sheep Dog to automatically insert photos into appropriate groups and recommend

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 5, May 2017

suitable tags for users on Flickr. They adopt concept detection to predict relevant concepts (tags) of a photo. Choudhury et al. proposed a recommendation framework to connect image content with communities in online social media. They characterize images through three types of features: visual features, user generated text tags, and social interaction, from which they recommend the most likely groups for a given image. Similarly, Yu et al. [42] proposed an automated recommendation system for a user's images to suggest suitable photo-sharing groups. Usage of social media's increased noticeably in today world facilitate the user to distribute their personal information like images with the other users. This enhanced technology leads to privacy disobedience where the users are allocated large volumes of images across additional number of people. To provide security for the information, mechanical explanation of images are introduced which aims to create the meta data information about the images by using the novel approach called Semantic interpret Markovian Semantic Indexing(SMSI) for repossess the images [1].

B. *Photo Privacy Algorithm:*

Input:
Workload (W) -> w1, w2, w3.....
Resource (RO) -> ro1, ro2, ro3...
Resource (RS) -> rs1, rs2, rs3…
Output: Migration (M)
Step 1: START
Step 2: Extract Total workload list W
Step 3: Access total Resource list RT
Step 4: Access total Resource list RW
Step 5: Set x=1, 2, 3……
Step 6: Look for RS(x) in W(x)
Step 7: Extract RS(x) from W(x)
Step 8: Access Type of RS(x) as T
Step 9: Look for RO(x) in W(x) of type T
Step 10: If found
Step 11: Extract Type of RO(x) as T1
Step 12: Set M = T1
Step 13: Else
Step 14: Set M = "Both"
Step 15: end

C. *Fake user detection :*

Input:
Workload (W) -> w1, w2, w3...
Resource (RT) (hint: Total number of friends)
Resource (RN) (hint: Total duration = CurrentDate – Date Of Join)
Resource (RF) (hint: Friend requests)
Output: Migration List (M) -> m1, m2, m3...
Step 1: START
Step 2: Extract Total workload list W
Step 3: Set x = 1, 2, 3…
Step 4: Extract RT from W(x).
Step 5: Extract RN from W(x).
Step 6: Extract list of RF from W(x).
Step 7: Count Workload list by grouping based on date
Step 8: Select MAX (Count)
Step 9: Set j = MAX (Count)
Step 10: Set k = (RT / RN)
Step 11: Set l = k/j

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 5, May 2017

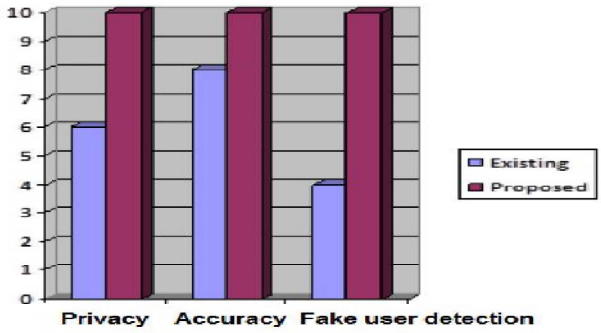
Step 12: Set M = l > 0? “Fake”: “Not fake”
Step 13: end

IV. PSEUDO CODE

Algorithm 1: Fake User Detection Algorithm
Step 1: Start
Step 2: User sending request to friend or family member then
Select
Case 1: Start sending out rampant friend requests just less than a week from accounts are created go to step 3
Case 2: User who get reported mostly as Fake Buddies user from multiple users go to step 4
Case 3: If the Buddies profile has less than two of his or her photo after a week from accounts are created go to step 5
Step 3: if (date difference <=7 and request count >=5) go to step 6
Step 4: if (fake user reported count >=5) go to step 6
Step 5: if (date difference >=7 and profile photo count <=2) go to step 6
Step 6: Fake user detected
Step 7: Show to receiver sender is fake user.
Step 8: Stop
Algorithm 2: Privacy Policy Algorithm
Step 1: Start
Step 2: User posting post
Select
Case 1: Post content match with friend library go to step 3
Case 2: Post content match with family library go to step 4
Case 3: Post content can`t match with friend or family library go to step 5
Step 3: if ((post content).equalsIgnoreCase(friend library)) then post for friend
Step 4: if ((post content).equalsIgnoreCase(family library)) then post for family
Step 5: else then post for friend and family (Public post)
Step 7: Show post to friend list or family list or Both (Public post).
Step 8: Stop

V. SIMULATION RESULTS

Here, Existing System taken image content for setting privacy policy for the input purpose but here author mainly focuses on Fake user detection based on abnormal activity parameters by which we are getting following result for our proposed system.



VI. CONCLUSION AND FUTURE WORK

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 5, May 2017

This paper we present a possible approach to reduce the communication of the Fake account profile Attack, where an enemy tries to impersonate a victim on an Online Social Network sites where the victim has no prior profile in place as well as privacy policy methods or techniques for user uploaded data photos in different content sharing network sites. Based on the user social behaviour and the user uploaded photos, the privacy policy can applied. Content based classification system is used, which supply users properly as well as easy, configured privacy setting for their uploaded image. Using this we can be easily prevent not only unwanted disclosure but also privacy violations. Unwanted disclosure may lead to misuse of one's personal data or information. The users automate the privacy policy settings for their uploaded images with the help of privacy policy fortune. On the basis of information available for a given user the system provides a expansive framework to infer privacy preferences and system is a practical tool.

REFERENCES

1. Mauro Conti, Radha Poovendran, Marco Secchiero FakeBook: Detecting Fake Profiles in University of Padua Via Trieste, 63 - Padua, Italy.
2. Sergej Zerr, Stefan Siersdorfer, Jonathon Hare, Elena Demidova, I Know What You Did Last Summer! : Privacy-Aware Image in L3S Research Center, Hannover, Germany.
3. P. F. Klemperer, Y. Liang, M. L. Mazurek, M. Sleeper, B. U. Lujo Bauer, L. F. Cranor, N. Gupta, M. K. Reitery Tag, You Can See It! Using Tags for Access Control in Photo Sharing in Carnegie Mellon University Pittsburgh, PA.
4. Mazzia,K. LeFevre and E. Adar,The PViz Comprehension Tool for Social Network Privacy Settingsin Photo Sharing in University of Michigan, Computer Science and Engineering,2260 Hayward Ave.Ann Arbor, MI 48109.
5. S.Jones and E.ONeill Contextual Dynamics of Group-Based Sharing De-cisionsin Department of Computer Science,University of Bath,Bath,BA2 7AY, UK.
6. Y.Liu,K.P.Gummadi,B.Krishnamurthy,A.Mislove Analyzing Facebook Privacy Settings:User Expectations vs. Reality in Northeastern University Boston,MA,USA.

BIOGRAPHY

Anant Mandre is a M.E Student in the Computer Engineering Department, JSPM's BSIOTR Wagholi College, Savitribai Phule Pune University. He received Bachelor Of Engineering (BE) degree in 2015 from Solapur University, Pandharpur, MS, India. His research interests are Data Mining.

Sonali Patil is a Assistant Professor in Computer Engineering Department, JSPM's BSIOTR Wagholi College, Pune, MS, India. She Pursuing her PHD from BSAU Chennai.