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. 4, Issue 12, December 2016

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, policy prediction 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.

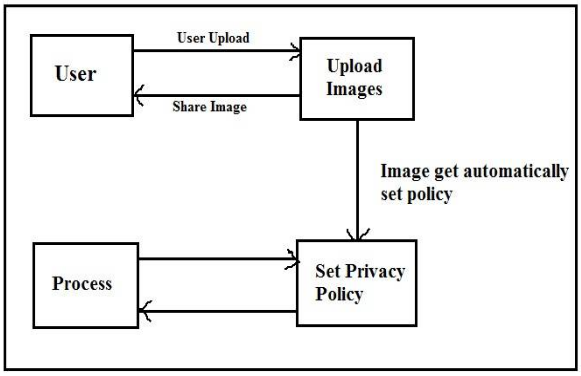
Hundreds of millions of people on Social Networking can swap their content through media, text like audio, video image etc. It will provides a content sharing mechanism and connects people across the global. The social media users can define a personal profile and change it as they wish. Through this 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.

DOI: 10.15680/IJIRCCE.2016. 0412218

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 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.

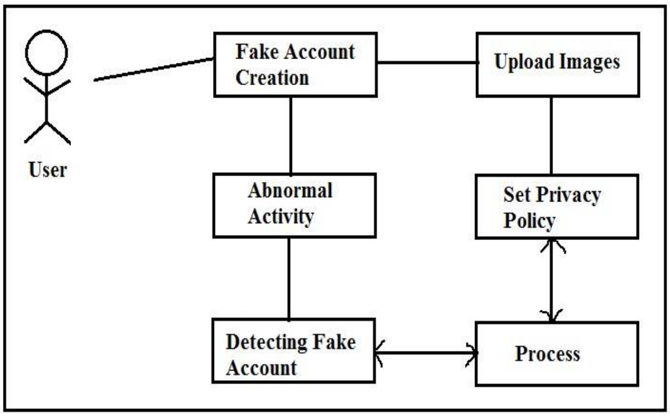
II. RELATED WORK

Existing System Architecture :



There are many websites like social networking sites where user should give the privacy preferences. But the research about the privacy preferences of user they suffers many problems to maintain their privacy settings and the main reason gives that the amount of shared information this process can be boring. So that, many have acknowledged the need of policy recommendation systems which can helps users to easily and properly configure privacy settings. However, existing proposals for automating privacy settings appear to be inadequate to address the unique privacy needs of images, due to the amount of information implicitly carried within images, and their relationship with the online environment wherein they are exposed.

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 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]. The proposed system automatically interprets the images using hidden Markov model and features are extorted by using colour histogram and Scale Invariant Feature Transform (SIFT) descriptor method. After interpreting these images, semantic retrieval of images can be done by using Natural Language using a tool named Word Net for measuring semantic comparison of annotated images in the database. Experimental results make available enhanced retrieval performance when evaluated with the existing system.

III. PROPOSED ALGORITHM

1) 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
```

2) 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
Step 12: Set M = l > 0? "Fake": "Not fake"
Step 13: end
```

V. SURVEY ON

1. **FakeBook: Detecting Fake Profiles in On-line Social Networks- Mauro Conti, Radha Poovendran, Marco Secchiero**
It gives 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. Privacy Suites is proposed by Jonathan Anderson
This allows users to easily choose ―suites" of privacy settings. Using privacy programming a privacy suite can be created by an expert. Privacy Suites could also be created directly through existing configuration UIs or exporting them to the abstract format. To the members of the social sites the privacy suite is distributed through existing distribution channels. Transparency is the main goal, which is essential for convincing influential users that it is safe to use.

3. **Privacy-Aware Image Classification and Search- Sergej Zerr**
This is a technique to automatically detect private images, and to enable privacy-oriented image search introduced by Sergej Zerr. To provide security policies technique combines textual meta data images with variety of visual features. It uses various classification models trained on a large scale dataset with privacy assignments obtained through a social annotation game. In this the selected image features (edges, faces, color histograms) which can help discriminate between natural and man-made objects/scenes (the EDCV feature) that can indicate the presence or absence of particular objects (SIFT).

4. **Privacy Policy Prediction (A3P)- Anna Cinzia Squicciarini**
This system is introduced by Anna Cinzia Squicciarini. Personalized policies can be automatically generated by this system. It makes use of the uploaded images by users and a hierarchical image classification is done. Images content and metadata is handled by the A3P system .It consists of two components: A3P Core and A3P Social. The

image will be first sent to the A3P-core, when the user uploads the image. The A3P-core classifies the image and determines whether there is a need to invoke the A3P-social. When meta data information is unavailable it is difficult to generate accurate privacy policy. This is the disadvantage of this system. Privacy violation as well as inaccurate classification will be the after effect of manual creation of meta data log information.

VI. CONCLUSION AND FUTURE WORK

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. A. 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.

DOI: 10.15680/IJIRCCE.2016. 0412218