*International Journal of scientific research and management (IJSRM)*
*\||Volume||3||Issue||5||Pages|| 2716-2720||2015||*
*Website: www.ijsrm.in ISSN (e): 2321-3418*

# Protection on Social Network Data Using Sensitive and Non-Sensitive Labels

***Prabhanjana Konni[1], Balaka Ramesh Naidu[2]***

[1]Aditya Institute of Technology and Management,
Tekkali, Srikakulam,Andhra Pradesh, India.
*09pm1f0023@gmail.com*

[2] Aditya Institute of Technology and Management,
Tekkali,Srikakulam,Andhra Pradesh, India.
*brn_balaka@yahoo.com*

**Abstract:** *This Paper is motivated by the recognition of the need for a finer grain and more personalized privacy in data publication of social networks. We propose a privacy protection scheme that not only prevents the disclosure of identity of users but also the disclosure of selected features in users' profiles, Labels are denoted either as sensitive or as non-sensitive. We treat node labels both as background knowledge an adversary may possess, and as sensitive information that has to be protected. To maintain the trustworthiness, We gather the authorized information as proof. In this Social Networking site We maintain privacy and also traceability whenever he/she breaks the protocol.*

**Keywords:** finer grain, Protocol, Trustworthiness, Traceability

## 1. Introduction

Nowadays social network data entails a privacy threat for their users. Sensitive information about users of the social networks should be protected[1]. The challenge is to devise methods to publish social network data in a form that affords utility without compromising privacy[2]. Previous research has proposed various privacy models with the corresponding protection mechanisms that prevent both inadvertent private information leakage and attacks by malicious adversaries. These early privacy models are mostly concerned with identity and link disclosure. The social networks are modeled as graphs in which users are nodes and social connections are edges. The threat definitions and protection mechanisms leverage structural properties of the graph. This paper is motivated by the recognition of the need for a finer grain and more personalized privacy. Users entrust social networks such as Face book and LinkedIn with a wealth of personal information such as their age, address, current location or political orientation. We refer to these details and messages as features in the user's profile. We propose a privacy protection scheme that not only prevents the disclosure of identity of users but also the disclosure of selected features in user's profile. An individual user can select the features of her profile which she wishes to conceal .The social networks are modeled as graphs in which users are nodes and features are labels[3].

Labels are denoted either as sensitive or as non-sensitive. Each node in the graph represents a user, and the edge between two nodes represents the fact that the two persons are friends. Labels annotated to the nodes show the locations of users. Each letter represents a city name as a label for each node. Some individuals do not mind their residence being known by the others, but some do, for various reasons. In such case, the privacy of their labels should be protected at data release. Therefore the locations are either sensitive or non-sensitive. The privacy issue arises from the disclosure of sensitive labels. One might suggest that such labels should be simply deleted. Still, such a solution would present an incomplete view of the network and may hide interesting statistical information that does not threaten privacy. A more sophisticated approach consists in releasing information about sensitive labels, while ensuring that the identities of users are protected from privacy threats. We consider such threats as neighborhood attack, in which an adversary _nds out sensitive information based on prior knowledge of the number of neighbors of a target node and the labels of these neighbors. for example, if an adversary knows that a user has three friends and that these friends are in A (Alexandria), B (Berlin) and C (Copenhagen), respectively, then she can infer that the user is in H (Helsinki). We present privacy protection

algorithms that allow for graph data to be published in a form such that an adversary cannot safely infer the identity and Although modeling features in the profile as attribute-value pairs would be closer to the actual social network structure, it is without loss of generality that we consider atomic labels.

For this purpose we design diversity-like model, where we treat node labels as both part of an adversary's background knowledge and as sensitive information that has to be protected. The algorithms are designed to provide privacy protection while losing as little information and while preserving as much utility as possible. We show that our solution is effective, efficient and scalable while offering stronger privacy guarantees than those in previous research, and that our algorithms scale well as data size grows.

## 2. Existing System

The current trend in the Social Network is not given any privacy about the user profile views. And also data sharing or (Posting) is taking more time and under the certain condition of displaying sensitive and non-sensitive data.

### 2.1 Problems on existing system:

1. There is no way to publish the Non sensitive data to all in social Network.
2. It's not providing privacy about user profiles.
3. Some mechanisms that prevent both inadvertent private information leakage and attacks by malicious adversaries.
4. Misuse of Information is done in the existing system because there is no trust worthiness and privacy check in traditional systems[6].

## 3. Proposed System

Here, we extend the existing definitions of modules and we introduced the sensitive or non-sensitive label concept in our project. We overcome the existing system disadvantages in our project[7].

### 3.1 Advantages:

1. We can publish the Non sensitive data to every-one in social Network.
2. It's providing privacy for the user profiles so that unwanted persons are not able to view your profiles[4].
3. We can post sensitive data to particular peoples and in the same way we can post non-sensitive data to everyone like ads or job posts.
4. Traceability and Privacy both are maintained in our social network site[5].

## 4. Implementation

Implementation is the stage of the project when the theoretical design is turned out into a working system. Thus it can be considered to be the most critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective. The implementation stage involves careful planning, investigation of the existing system and it's constraints on implementation, designing of methods to achieve changeover and evaluation of changeover methods.

### 4.1 Main Modules

**User Module:**

In this module, Users are having authentication and security to access the detail which is presented in the ontology system. Before accessing or searching the details user should have the account in that otherwise they should register first.

**Information Loss:**

We aim to keep information loss low. Information loss in this case contains both structure information loss and label information loss. There are some non sensitive data's are Loss due to Privacy making, so, we can't send out full information to the public.

**Sensitive Label Privacy Protection:**

There are who post the image to the online social network if allow the people for showing the image it will display to his requesters it make as the sensitive to that user. This is very useful to make sensitive data for the public .

## 5. Results

Check **OracleServiceXE**,**OracleXETNSListen** service.msc whether it is started on not. If not start it.

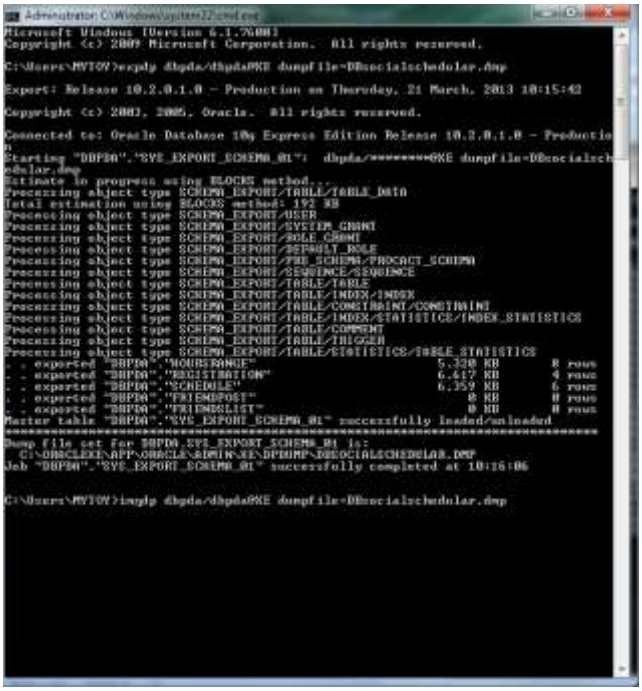



**Figure 1:**Oracle Service,XE Installation

**LOGIN PROCESS**

- The below screen shot shows the authenticated user to login with their user name and password.
- If it's a new user, we need to be authenticated by pressing RegisterNow which is given below the user name and password[8].

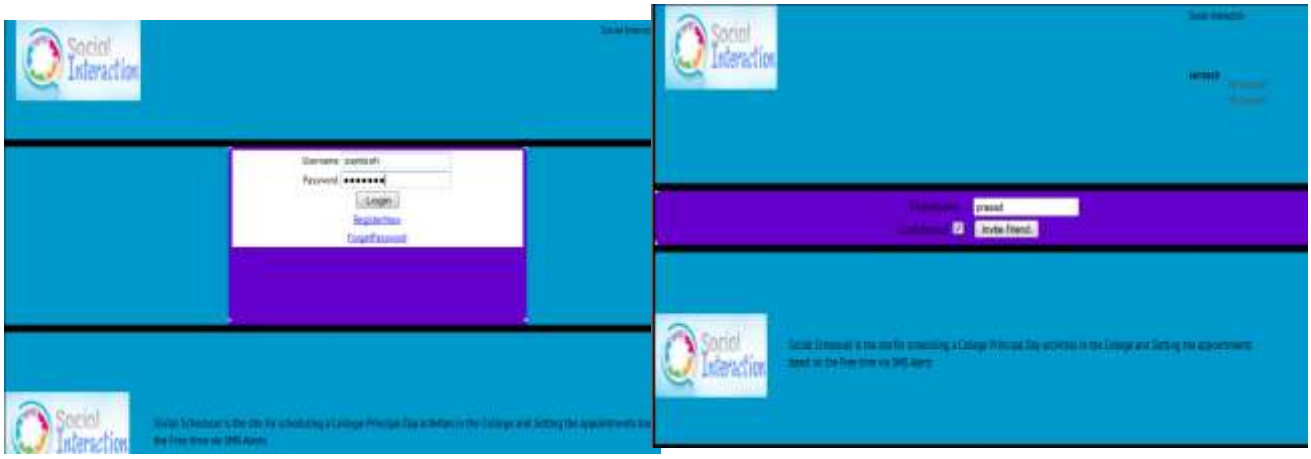


**Figure 2:** Login Process

**USER PROFILE**

- The below screen shot shows that, the display of a picture which has been posted by the friends.
- This can be seen by all the members as per mentioned either it's a confidential or non confidential[9].

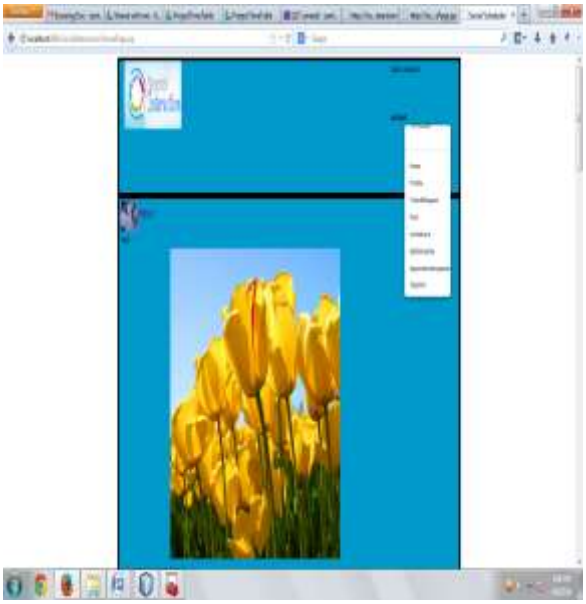


**Figure 3:** User profile

**REQUEST TO A FRIEND**

- The below screen shot displays the process of sending friend request.
- The friend name should be entered in the asked space.
- And also need to be marked either confidential or not.
- Then press invite friend, thus a friend request is sent.



**Figure 4:** Request to a Friend

**SHARING DATA**

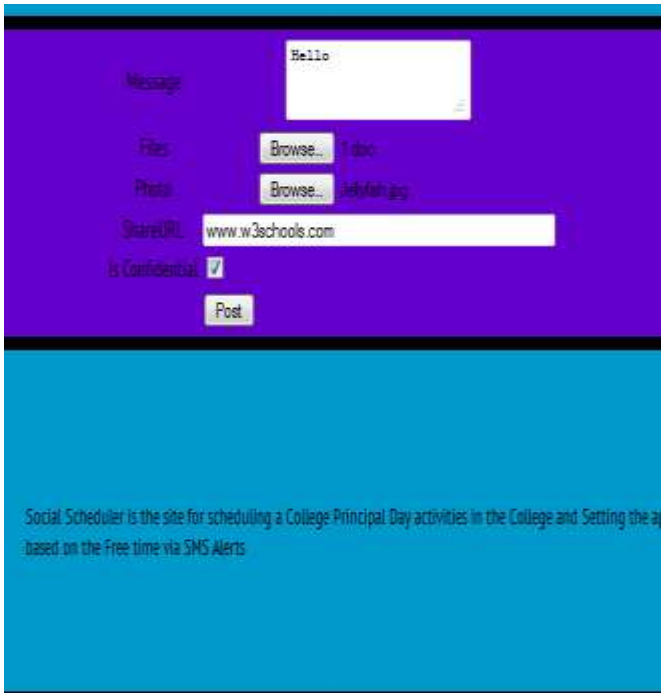
The screen shot displays the, options of data been shared by the friends.

- Message can be sent and along with it many more like file, photo, url, which can be attained by browsing from the system either by web or internal.
- Then need to mark it as confidential or not. Then press post , so that data gets shared[10]

**Figure 5:**Sharing Data

**OTHER USER ACCEPT THE REQUEST**

- . The screen shot shows that, when an invitation has




been sent it displays in this way.

- If you wanted to accept it we need to press on accept button given below.
- And place the friendliest in either confidential or non confidential.

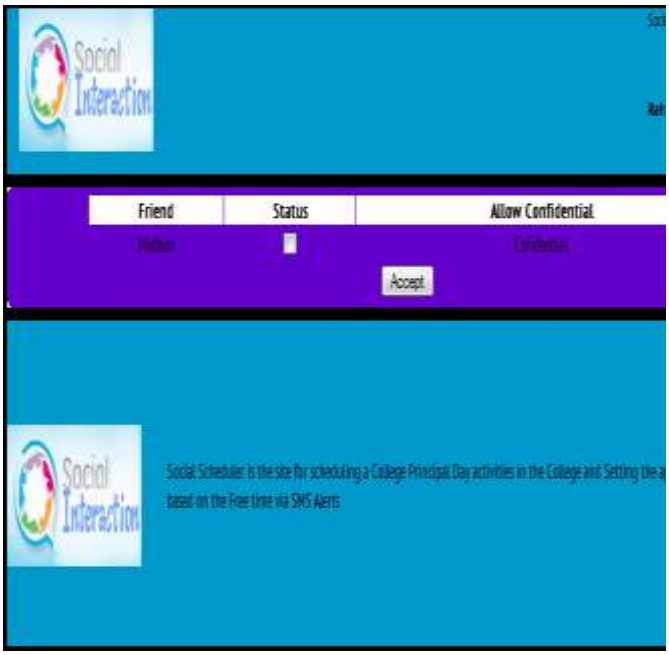



**Figure**.6: Other User Accept the Request

**DISPLAY OF STATUS**

- The screen shot displays that when a invitation sent to user the option to be done are two ways either to accept it or ignore it.
- The invitation sent to you comes along with date and content.
- If the invitation is accepted the flag become Y if not N.(yes or no).
- Thus it shows the status of the user.

**SIGN OUT**


**Figure**7 Display of Status

After performing all tasks the user will SIGN OUT.

## Conclusion

In this paper we introduce investigated the protection of private label information in social network data publication. The data is categorized to be either sensitive or non-sensitive. We assume that adversaries possess prior knowledge about a node's degree and the labels of its neighbors, and can use that to infer the sensitive labels of targets. We propose a privacy protection scheme that not only prevents the disclosure of identity of users but also the disclosure of selected features in users' profiles. To maintain the Trustworthiness we gather the authorized information as proof. In this Social Networking site we Maintain Privacy and also Traceability whenever he/she break the protocol

## References


[1] A. Bonnaccorsi, "On the Relationship between Firm Size and Export Intensity," Journal of International Business Studies, XXIII (4), pp. 605-635, 1992. (journal style)

[2] R. Caves, Multinational Enterprise and Economic Analysis, Cambridge University Press, Cambridge, 1982. (book style)

[3] M. Clerc, "The Swarm and the Queen: Towards a Deterministic and Adaptive Particle Swarm Optimization," In Proceedings of the IEEE Congress on Evolutionary Computation (CEC), pp. 1951-1957, 1999. (conference style)

[4] H.H. Crokell, "Specialization and International Competitiveness," in Managing the Multinational Subsidiary, H. Etemad and L. S, Sulude (eds.), Croom-Helm, London, 1986. (book chapter style)

[5] K. Deb, S. Agrawal, A. Pratab, T. Meyarivan, "A Fast Elitist Non-dominated Sorting Genetic Algorithms for Multiobjective Optimization: NSGA II," KanGAL report 200001, Indian Institute of Technology, Kanpur, India, 2000. (technical report style)

[6] J. Geralds, "Sega Ends Production of Dreamcast," vnunet.com, para. 2, Jan. 31, 2001. [Online]. Available: http://nl1.vnunet.com/news/1116995. [Accessed: Sept. 12, 2004]. (General Internet site)

[7] A. G. Francesco Bonchi and T. Tassa. Identity obfuscation in graphs through the information theoretic lens. In ICDE, 2011.

[8] M. Hay, G. Miklau, D. Jensen, D. Towsley, and P. Weis. Resisting structural re-identi_cation in anonymized social networks. PVLDB, 1(1), 2008.

[9] Y. Li and H. Shen. Anonymizing graphs against weight-based attacks. In ICDM Workshops, 2010.

[10] K. Liu and E. Terzi. Towards identity anonymization on graphs. In SIGMOD,2008.


.