International Journal of Research in Advent Technology (IJRAT) Special Issue
E-ISSN: 2321-9637
Available online at www.ijrat.org
National Conference on "Role of Information Technology in Social Innovations"
26th & 27th February 2019

Managing Different User's Privacy Issues on Social Media

Mr.A.J.Patankar[1], Neha Chiddarwar[2], Mayuri Kulkarni[3], Chaitali Kulkarni, Dr.Kotrappa Sirbi, Sayali Kharche[5]
Department Professor. Dept. Information [1], .B.E. Dept. Information Technology, DYPCOE[2,3,4,5] , SPPU, Pune[1,2,3,4,5]
Email: abhijitpatankarmail@gmail.com[1]

Abstract-Basically an online social network focused on many people's profile to spend time on an online social network, also implementing OSN client's social circles, by using recommended suggestions. In this system, the main focus is on globalization has increased beyond its growth, many challenges and stressful situations need to be faced by human. And also we are Recommendation for single OSN model. Facebook is used by many people around world. User can publish their own detail and can contact with their friends. This information is private. Because of this structure clients can easily contact with their friends. The project aims at creating a social networking for people. We also want to provide them with all the facilities for better and secure communication among them. Basically, it will let the user to choose the right person he/she is contacting to. It will also preserve the privacy of its users' profiles which is sensitive. And hide the sensitive information.

Index Terms- User Privacy, Social Media

1. INRTODUCTION

Private information leakage could be an important issue in some cases. And explore how to launch inference attacks using released social networking data to predict private information. In this we map this issue to a collective classification problem and propose a collective inference model. In our model, an attacker utilizes user profile and social relationships in a collective manner to predict sensitive information of related victims in a released social network dataset. To protect against such attacks, we propose a data sanitization method collectively manipulating user profile and friendship relations. The key novel idea lies that besides sanitizing friendship relations, the proposed method can take advantages of various data-manipulating methods. We show that we can easily reduce adversary's prediction accuracy on sensitive information, while resulting in less accuracy decrease on non-sensitive information towards three social network datasets. To the best of our knowledge, this is the first work that employs collective methods involving various data-manipulating methods and social relationships to protect against inference attacks in social networks. Privacy concerns in social networks can be mainly categorized into two types: inherent-data privacy and latent data privacy. Inherent-data privacy is related to sensitive data contained in the data profile submitted by users in order to receive data-related services.

2. LITERATURE SURVEY

2.1. *curso: Protect Yourself from Curse of Attribute Inference*

Whether Alice's sensitive attribute can be inferred based on public information in Alice's neighborhood, and Whether making Alice's sensitive attribute public leads to the disclosure of sensitive information of another user Bob in Alice's neighborhood. You Are Who You Know: Inferring User Profiles in Online Social Networks.

2.2. *Lists of items Wherefore Art Thou R3579X? Anonymized Social*

In an effort to preserve privacy, the practice of anonymization replaces names with meaningless unique identifiers. We describe a family of attacks such that even from a single anonymized copy of a social network, it is possible for an adversary to learn whether edges existor not between specific targeted pairs of nodes.

3. FUTURE SCOPE

The system is about developing an online social network which provides more secure privacy of a user's profile. The system also deals with developing a mechanism to provide users with secure communication.

3.1. *Proposed System*

In this paper, we focus on latent-data privacy. We assume third party users may collect anonymous user data from social networks. Some users disclose their sensitive information, while others do not. However, third party users can carry out de-anonymization actions and further infer sensitive information of users. We first investigate how to infer sensitive information hidden in the released data. Then, we propose some effective data sanitization strategies to prevent information inference attacks. On the other hand, the sanitized data obtained by these strategies should not reduce the valuable benefit brought by the abundant data resources, so that non-sensitive information can still be inferred and utilized by third party users. To launch an inference attack by third party users, we employ a typical inference attack, called collective inference, as a case study. We present a novel implementation method for collective inference. Collective inference mainly rely on iteratively propagating current predicting results throughout a network to improve prediction accuracy, thus we need to consider how to best predict sensitive information in each iteration.

3.1.1. ***Advantages of Proposed System***

1. Find large number of attacks in social networks.
2. Proposed system can manage privacy and data utility in social network.
3. Anonymous users cannot obtain private information to accurately predict sensitive information.
4. Special features of social network data to investigate collective attacks in diverse large scale social networks.

3.2. *SYSTEM SPECIFICATION*

- **Hardware Specification**
  - Processor: Pentium IV 2.4 GHz.
  - Hard Disk: 40 GB.
  - Monitor: :15VGA
  - Mouse:: Logitech.
  - Ram: Min 256 Mb
- **Software Specification**
  - Operating system: Windows XP/7
  - Coding Language: JAVA/J2EE, Hibernate.
  - IDE: Java eclipse.
  - Web server: Apache Tomcat 7.
  - Front End: JSP, CSS etc.
  - Back End: MySQLas database server.

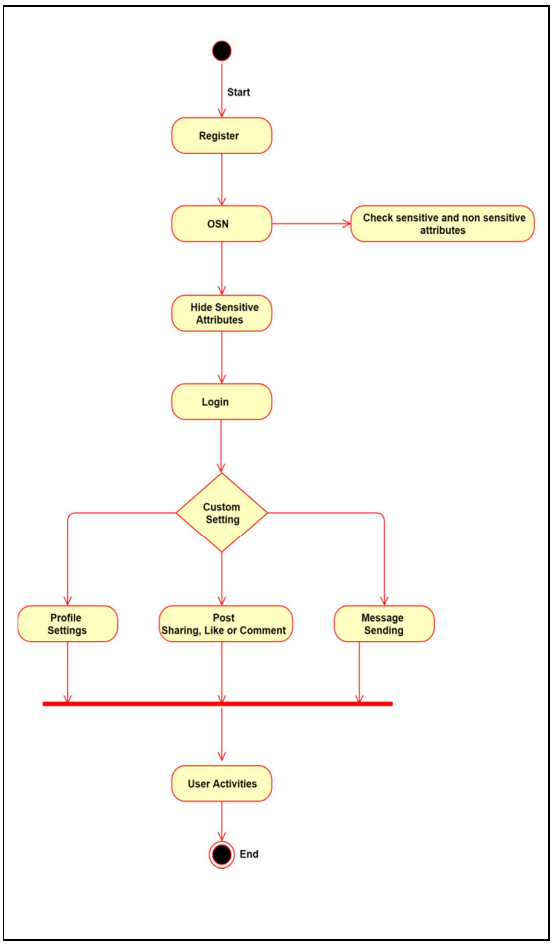


Fig. 1. Activity Diagram

3.3. *System Design*

4. Algorithms

4.1. *Mathematical Model*

Let W be the whole system which consists: W= {IP, PRO, OP}Where,

IP is the input of the system.

A) IP= {U, C, R, OSN, SA, UA}

1. U is the number of users in the system.
2. R is the set of number of registered U in the system.

3. C is the custom setting for all U.
4. OSN is the system.
5. SA is the sensitive attributes.
6. UA is the User Activities.

4.2. *Naïve Bayes Algorithm Steps:*

Step 1: It is loaded the text file which will be classified as being ONE, TWO or THREE
Step 2: There are loaded the text file found in the folder **.**
The name of the files belonging to class ONE are:"abc_.txt", the ones belonging to class TWO are: "pqr_.txt" and the ones for class THREE are : "xyz_.txt".
Step3: It is determined the a priori probability for each class: P(UNU) = NrTemplateInClassONE / NumberTotalTemplates
P(DOI) = NrTemplateInClassTWO / NumberTotalTemplates
P(TREI) = NrTemplateInClassTHREE / NumberTotalTemplates
Step 4: It is determined the probability that the text file from the Step 1 to be in class ONE, TWO or THREE. Let (i,j) be the position of a attribute in the text file. It is calculated the probability that the attribute having the coordinates (i, j) to be for the class ONE, TWO and THREE.
count1i,j = 0
for k = 1,n ; n – the number of attribute in class ONE if abc_k(i,j) = 255 then
count1i,j = count1i,j + 1
probability1(i,j) =count1i,j / NrTemplateInClassONE count2i,j = 0
for k = 1,n ; n- the number of attribute in class TWO

if pqr_k(i,j) = 255 then
count2i,j = count2i,j + 1
probability2(i,j) =count2i,j / NrTemplateInClassTWO count3i,j = 0
for k = 1,n ; n- the number of attribute in class THREE if xyz_k(i,j) = 255 then
count3i,j = count3i,j + 1
probability 3(i,j) =count3i,j / NrTemplateInClassTHREE
Step 5.
The posteriori probability that the attribute in Step 1 to be in class ONE is:
P(T|ONE) = average (probabilitate1(i,j)); (i, j) – the position of the attribute in the text file from Step1
Step 6.
The posteriori probability that the attribute in Step 1 to be in class TWO is:
P(T|TWO) = average (probabilitate1(i,j)); (i, j) – the position of the attribute in the text file from Step1
Step 7:
The posteriori probability that the attribute in Step 1 to be in class THREE is:
P(T|THREE) = average (probabilitate1(i,j)); (i, j) – the position of the attribute in the text file from Step1
Step 8:
It is determined the probability P for each text file class and it is assigned the text file from Step1 to the class of text file that has the greatest probability.
P(ONE|T) = P(T| ONE)*P(ONE)
P(TWO|T) = P(T| TWO)*P(TWO)
P(THREE|T) = P(T| THREE)*P(THREE)

4.3. *PRO is the procedure of our proposed system*

List Step 1: At first user will register into the OSN system with his/her basic information.
Step 2: The registered information will be forwarded to OSN system.
Step 3: OSN system will check the sensitive and non- sensitive attributes of registered users.
Step 4: OSN system will automatically hide the sensitive Information system.
Step 5:Then user will login into the system.
Step 6: User will perform the UA like profile setting, post sharing, like or comment onto the post and message sending to the another users by matching the attributes.
Step 7: Then OSN will provide the privacy for users likes and comments post.

OP is the output of the system:
The system provides the privacy to the user's sensitive data and privacy for posts which share by users.

A. Modules.

1. User
2. OSN System

1. User

- Registration
- Login
- Post Status
- Profile setting
- Send message to another users

- Logout

A. Registration

The user will register to the system with normal information. At the time of registration the OSN system will hide the user's sensitive information

B. Modules

For login to the system, user will enter the Username and password, if entered details are correct then the system will redirect him to home page otherwise it will shows an error message.

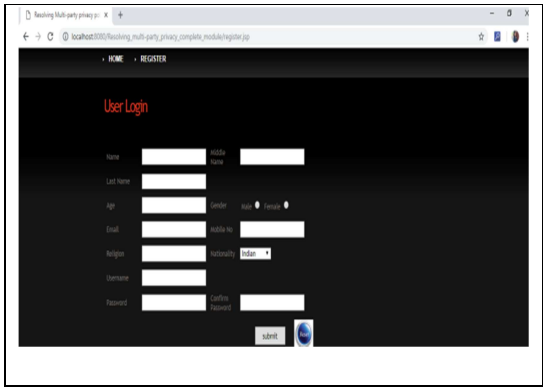
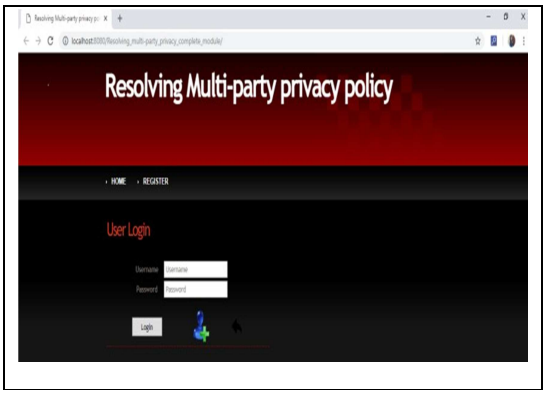


Fig. 2 Login page



C. Logout

User logout the account from system.

The OSN system:

- Check sensitive and non-sensitive information of all users
- Check the all registered users sensitive information.
- It stored the sensitive attributes.
- The OSN will provide the privacy for users like and comments posts.

5. Mathematical model

Relevant mathematics associated with the Project

Let W is the Whole System Consists:

W= {IP, PRO, OP}
Where,

IP is the input to the system IP = {U, S, C, B, R, r,F} *Where,*

1. U is the set of number users.

   U = {U1; U2::::Un}
2. S is the system which contains the unstructured data to provide the service to user based on user request.
3. C is set of number of cluster based on user request. C = {C1; C2; Cn}:

4. B be set of bloom filter which is required to filter the user requests based on user interest.

5. F be the set of files user is requesting.

   F = {f1, f2..... fn}.

6. R be the user request for file to S.

7. r be the rank assigned to le based user request.

Acknowledgments

We have taken efforts in this project, however, it would not have been possible without the kind support and help of many individuals and organizations. We would like to extend our sincere thanks to all of them. We are highly indebted to Mr.A.J.Patankar for his guidance and constant supervision as well as for providing necessary information regarding the project & also for his support in completing the project. We would like to express our gratitude towards our parents & our Head of I.T. Department Dr.PreetiPatil for their kind co-operation and encouragement which helped us in completion of this project. Furthermore, I would also

like to acknowledge with much appreciation the crucial role of the staff of DYPCOE Akurdi, who gave the permission to use all required equipment and the necessary materials to complete my project stage I. We are also deeply grateful to the Principal of DYPCOE ,Dr.VijayWadhai and my parents for their financial and logistical support and for providing necessary guidance concerning project's implementation.

REFERENCES

[1] L. Backstrom, C. Dwork, and J. Kleinberg. Wherefore art thou r3579x?: Anonymized social networks, hidden patterns, and structural steganography. In Proceedings of the 16th International Conference on World Wide Web, WWW '07, pages 181–190, New York, NY, USA, 2007. ACM.

[2] M. Balduzzi, C. Platzer, T. Holz, E. Kirda, D. Balzarotti, and C. Kruegel. Abusing social networks for automated user profiling. In Recent Advances in Intrusion Detection, pages 422–441. Springer, 2010.

[3] M. Bayati, M. Gerritsen, D. F. Gleich, A. Saberi, and Y. Wang. Algorithms for large, sparse network alignment problems. In Data Mining, 2009. ICDM'09. Ninth IEEE International Conference on, pages 705–710. IEEE, 2009.

[4] O. Berthold, A. Pfitzmann, and R. Standtke. The disadvantages of free mix routes and how to overcome them. In Designing Privacy Enhancing Technologies, pages 30–45.Springer,2000