www.ijecs.in

International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 3 Issue 6 June, 2014 Page No. 6726-6728

Avoid personal data presumption attacks on social networks

T. Swetha, V. Balaji, P.Nirupama

M.Tech: Department of CSE SIETK, Puttur, INDIA
swethathammisetty7@gmail.com

Assistant Professor
Department of CSE SIETK, Puttur, INDIA
vuppala.balaji@gmail.com

Head of the department
Department of CSE SIETK,Puttur,INDIA

Abstract- Now a day's many people are rapidly increases the use of social networks like facebook. By using these networks so many number of users are connected with their friends and relatives. Some of the user related data should be private in the networks. To launch presumption attacks using released social networking data to forecast personal data. Three possible refining techniques that could be used in different situations. Discover the effectiveness of these techniques and challenge to use methods of collective presumption to discover sensitive attributes of the data set. So then decrease the effectiveness of both local and relational classification algorithms by using the sanitization methods can describe.

Keywords- Social network analysis, data mining, social network privacy;

I. RELATED WORK

Touch on many areas of examine that have been studied. The area of privacy inside a social network encompasses a large span, based on how privacy is defined. Due to their freedom of pre-existing infrastructure and pre-configuration there exists many problems. Some of them are solved as explained below.

L. Backstrom, C. Dwork, and J. Kleinberg [1] consider a way in a social network, nodes correspond to people or other social entities, and edges keep in touch to social links between them. In an stab to preserve privacy, the practice of anonymization replaces names with meaningless single identifiers. Describe a family of attacks such that even from a single anonymzed copy of a social network, it is possible for an adversary to learn whether edges exist or not between specific besieged pairs of nodes.

M. Hay, G. Miklau, D. Jensen, P. Weis, and S. Srivastava. [2] Operators of online social networks are more and more sharing potentially perceptive information about users and their relationships with advertisers, appliance developers, and data-mining researchers. Privacy is typically secluded by anonymization, i.e., removing names, addresses, etc. Present a structure for analyzing privacy and anonymity in social networks and develop a new re-identification algorithm target anonymized social-network graphs. To express its helpfulness on real-world networks, we show that a third of the users who can be verified to have accounts on both Twitter, a popular micro blogging service, and Flickr, an online photo-sharing site, can be re-identified in the anonymous Twitter graph with only a 12% error rate. Our de-anonymization algorithm is based purely on the network topology, does not require creation of a large number of dummy "sybil" nodes, is robust to din and all existing lines, and works even when the overlap between the target network and the adversary's back up information is small.

K. Liu and E. Terzi. [3] The increase of network data in various application domains has raised privacy concerns for the persons involved. Recent studies show that simply removing the identities of the nodes before publishing the graph/social network data does not security privacy. The structure of the graph itself, and in its basic form the degree of the nodes, can be informative the identities of folks. To address this issue, study a specific graph-anonymization problem. Call a graph *k*-degree unidentified if for every node *v*, there exist at least *k*-1 other nodes in the graph with the same degree as *v*. This classification of secrecy prevents the re-identification of persons by adversaries with *a priori* knowledge of the degree of certain nodes. Formally define the graph-anonymization problem that, given a graph *G*, asks for the *k*-

degree unspecified graph that stems from *G* with the lowest number of graph-modification operations. Create simple and well-organized algorithms for solving this problem.

J. He, W. Chu, and V. Liu. [4] Currently, millions of individuals are sharing personal information and building social relations with others, throughout online social network sites. Recent research has shown that personal information could compromise owners' privacy. involved in the privacy of online social network users with missing personal information. Study the problem of inferring those users' personal information via their social associations. Present an iterative algorithm, by combining a Bayesian label classification method and discriminative social relation choosing, for inferring personal information. Personal information of most users in an online social network could be inferred through simple social relations with high accuracy.

E. Zheleva and L. Getoor. [5] trouble of preserving the privacy of sensitive relationships in graph data. Refer to the problem of inferring sensitive relationships from anonymized graph data as *link re-identification*. Five different privacy preservation strategies, which vary in terms of the amount of data removed (and hence their utility) and the amount of privacy preserved. Assume the antagonist has an accurate predictive model for links, and the success of different link re-identification strategies under unreliable structural characteristics of the information.

Raymond Heatherly, Murat Kantarcioglu, and Bhavani Thuraisingham, Fellow,[6] consider a way for preserving privacy Information Inference Attacks on Social Networks focuses on the problem of private information leakage for individuals as a express result of their actions as being part of an online social network. Model an attack situation as follows: Suppose Facebook desires to release data to electronic arts for their use in advertising games to fascinated people. However, once electronic arts have this data, they want to discover the political affiliation of users in their data for lobbying efforts. Because they would not only use the names of those persons who explicitly list their affiliation, but also—throughout inference—could establish the affiliation of other users in their information, this would obviously be a privacy infringement of hidden details.

Here we propose the major issues concerning privacy and security in online social networks. That aims to protect user data from the various attack vantage points including other users, advertisers, third party application developers, and the online social network source itself. Next cover social network inference of user attributes, locating hubs, and link prediction. Some of the user related data should be private in the networks. To launch presumption attacks using released social networking data to forecast personal data. Three possible refining techniques that could be used in different situations. Discover the effectiveness of these techniques and challenge to use methods of collective presumption to discover sensitive attributes of the data set. So then decrease the effectiveness of both local and relational classification algorithms by using the sanitization methods can describe.

II INTRODUCTION

Social networks are online applications that allow their users to connect by way of various link types. These offerings, allow people to connect their friends and list information about themselves that are relevant to the network. For example, Facebook is a general-use social network, so single users list their desired activities, books, and movies. In opposition, LinkedIn is a professional network; because of this, users specify details which are related to their professional life (i.e., reference letters, previous employment, and so on.) Because these sites collect extensive personal information, social network application providers have a rare opportunity: direct use of this information could be useful to advertisers for direct advertising. Privacy concerns can prevent these efforts [7]. This conflict between the desired use of data and individual privacy presents an opportunity for privacy-preserving social network data mining—that is, the discovery of information and associations from social network data without contravene privacy. Privacy concerns of individuals in a social network can be classified into two categories: privacy after data release, and private information leakage.

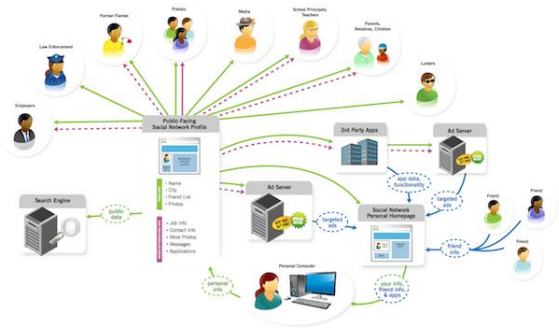

Figure 1: Social network system

Instances of privacy after data release involve the identification of specific folks in a data set subsequent to its discharge to the general public or to paying customers for a specific usage.

Private information leakage is related to details about an individual that are not clearly accepted, but, rather, are incidental through other details released and/ or relationships to individuals who may express that detail. A small example of this type of information leakage is a situation where a user, say John, does not enter his political connection because of privacy concerns. Here mainly focuses on the problem of private information leakage for individuals as a direct result of their actions on online social network. We model an attack setting as follows: Suppose Facebook wishes to release data to electronic arts for their use in promotion games to fascinated people. Once electronic arts have these facts, they want to identify the political connection of users in their data for lobbying efforts. Because they would not only use the names of those individuals who explicitly list their affiliation, but also through inference could determine the affiliation of other users in their data, this would obviously be a privacy infringement of hidden details. Explore how the online social network data could be used to predict some individual private detail that a user is not willing to disclose (e.g., sexual orientation) and explore the effect of possible data sanitization approaches on prevent such personal information leakage, while allowing the addressee of the sanitized data to do inference on no private details.

This problem of private information leakage could be an main issue. Recently, both ABC News [8] and the Boston Globe [9] published reports indicative of that it is possible to determine a user's sexual orientation by obtaining a relatively small sub graph from Facebook that includes only the user's gender, the gender they are interested in, and their friends in that sub graph. Forecast an individual's sexual orientation or some other personal detail may seem like inconsequential, but in some cases, it may create negative repercussions (e.g., discrimination,
and so on.).

III TECHNIQUES USED

Three possible sanitization techniques that could be used in various situations. Then, explore the effectiveness of these techniques and attempt to use methods of collective inference to discover sensitive attributes of the data set. Because decrease the effectiveness of both local and relational classification algorithms by using the sanitization methods we described. And the network classification description is shown below.

Network Classification

Collective inference is a method of classifying social network data using a grouping of node details and connecting links in the social graph. Each of these classifiers consists of three components: They are as follows:

1. Local Classifiers
2. Relational Classifiers
3. Collective Inference Methods

A. Local Classifiers

It is a classification technique that examines details of a node and constructs a classification scheme. This classifier builds a model based on the details of nodes in the training set. Here only shows details of one node.

B. Relational Classifiers

The relational classifier is a separate type of knowledge algorithm that looks at the link structure of the graph. It describes the node to node relation link.

C. Collective Inference Methods

Local classifiers consider only the details of the node it is classifying. Equally, relational classifiers consider only the link structure of a node. Specifically, a main problem with relational classifiers is that while we may smartly divide fully labeled test sets so that we ensure every node is connected to at least one node in the training set, real-world data may not gratify this strict requisite. If this requirement is not met, then relational classification will be unable to classify nodes which have no neighbors in the training set. Collective inference attempts to make up for these deficiencies by using both local and relational classifiers in a accurate manner to attempt to increase the classification precision of nodes in the network.

IV. CONCLUSION

Addressed various issues related to private information leak in social networks. By using both friendship links and details jointly gives better obviousness than details alone. The effect of removing details and links in preventing responsive information leakage. Here discovered situations in which collective inference does not improve on using a simple local arrangement method to identify nodes. When merge the results from the collective inference implications with the person results, begin to see that removing details and friendship links together is the best way to decrease classifier accuracy. This is probably infeasible in maintaining the use of social networks. That by removing only details, we greatly reduce the correctness of local classifiers, which give us the maximum exactness that were able to achieve through any grouping of classifiers. Also assumed full use of the graph information when deciding which details to hide. Useful research could be done on how individuals with limited access to the network could pick which details to hide.

REFERENCES

[1] L. Backstrom, C. Dwork, and J. Kleinberg, "Wherefore Art Thou r3579x?: Anonymized Social Networks, Hidden Patterns, and Structural Steganography," Proc. 16th Int'l Conf. World Wide Web (WWW '07), pp. 181-190, 2007.

[2]M. Hay, G. Miklau, D. Jensen, P. Weis, and S. Srivastava, "Anonymizing Social Networks," Technical Report 07-19, Univ. of Massachusetts Amherst, 2007.

[3]K. Liu and E. Terzi, "Towards Identity Anonymization on Graphs," Proc. ACM SIGMOD Int'l Conf. Management of Data (SIGMOD '08), pp. 93-106, 2008.

[4]J. He, W. Chu, and V. Liu, "Inferring Privacy Information from Social Networks," Proc. Intelligence and Security Informatics, 2006.

[5]E. Zheleva and L. Getoor, "Preserving the Privacy of Sensitive Relationships in Graph Data," Proc. First ACM SIGKDD Int'l Conf. Privacy, Security, and Trust in KDD, pp. 153-171, 2008.

[6] Raymond Heatherly, Murat Kantarcioglu, and Bhavani Thuraisingham, Fellow, consider a way for preserving privacy Information Inference Attacks on Social Networks 2013.

[7] Facebook Beacon, 2007.

[8] K.M. Heussner, "'Gaydar' n Facebook: Can Your Friends Reveal Sexual Orientation?" ABC News, http://abcnews.go. Com/Technology/gaydar-facebook-friends/story?id=8633224#. UZ939UqheOs, Sept. 2009.

[9] C. Johnson, "Project Gaydar," The Boston Globe, Sept. 2009.