ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Predicting Private Information and Detecting inference Attacks on Social Networks Data

K.Laxman
Department of Computer Science & Engineering,
Vignan College of Engineering, Kondapur, Medchel, Hyderabad, Telangana - 501401, India.

N.Shanker
Department of Computer Science & Engineering,
Nizam College, Basheer Bagh, Hyderabad, Telangana - 500001, India.

P. Vamshi
Department of Computer Science & Engineering,
Vignana Bharathi Institute of Technology, Ghatkesar, Hyderabad, Telangana – 501301, India.

Abstract:
Online social networks, such as Facebook, are increasingly utilized by many people. These networks allow users to publish details about themselves and to connect to their friends. Some of the information revealed inside these networks is meant to be private. Yet it is possible to use learning algorithms on released data to predict private information. In this paper, we explore how to launch inference attacks using released social networking data to predict private information. We then devise three possible sanitization techniques that could be used in various situations. Then, we explore the effectiveness of these techniques and attempt to use methods of collective inference to discover sensitive attributes of the data set. We show that we can decrease the effectiveness of both local and relational classification algorithms by using the sanitization methods we described.

EXISTING SYSTEM:

Other papers have tried to infer private information inside social networks. In, He et al. consider ways to infer private information via friendship links by creating a Bayesian network from the links inside a social network. While they crawl a real social network, Live Journal, they use hypothetical attributes to analyze their learning algorithm. The existing work could model and analyze access control requirements with respect to collaborative authorization management of shared data in OSNs [1]. The need of joint management for data sharing, especially photo sharing, in OSNs has been recognized by the recent work provided a solution for collective privacy management in OSNs. Their work considered access control policies of a content that is co-owned by multiple users in an OSN, such that each co-owner may separately specify her/his own privacy preference for the shared content [3].

DISADVANTAGES OF EXISTING SYSTEM:

This problem of private information leakage could be an important issue in some cases.

PROPOSED SYSTEM:

This paper focuses on the problem of private information leakage for individuals as a direct result of their actions as being part of an online social network. We model an attack scenario as follows: Suppose Facebook wishes to release data to electronic arts for their use in advertising games to interested people. However, once electronic arts has this data, they want to identify the political affiliation of users in their data for lobbying efforts [5],[14]. 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 violation of hidden details. We 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., political or religious affiliation, sexual orientation) and

Cite this article as: K.Laxman, N.Shanker & P.Vamshi, "Predicting Private Information and Detecting inference Attacks on Social Networks Data", International Journal & Magazine of Engineering, Technology, Management and Research, Volume 4 Issue 11, 2017, Page 174-177.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

explore the effect of possible data sanitization approaches on preventing such private information leakage, while allowing the recipient of the sanitized data to do inference on non-private details. In Proposed System we implemented a proof-of-concept Facebook application for the collaborative management of shared data, called MController. Our prototype application enables multiple associated users to specify their authorization policies and privacy preferences to co-control a shared data item [2].

ADVANTAGES OF PROPOSED SYSTEM:

To the best of our knowledge, this is the first paper that discusses the problem of sanitizing a social network to prevent inference of social network data and then examines the effectiveness of those approaches on a real-world data set [4]. In order to protect privacy, we sanitize both details and the underlying link structure of the graph. That is, we delete some information from a user's profile and remove some links between friends. We also examine the effects of generalizing detail values to more generic values [12],[13].

IMPLEMENTATION MODULES:

1. Privacy clarity for Formal data
2. Control of data's
3. Choosing of details Module
4. Operate Link Information
5. Generalization Module

MODULES DESCRIPTION:

1. Privacy Clarity for Formal data:

In this module we develop the privacy clarity of formal data where, Privacy definition could be applied to other domains. Consider the scenario where we want to decide whether to release some private information (e.g., eating habits, lifestyle), and combined with some public information (e.g., age, zip code, cause of death of ancestors) or not [10]. We may be worried that whether the disclosed information could be used to build a data mining model to predict the likelihood of an individual getting an Alzheimer's disease. Most individuals would consider such information to be sensitive for example, when applying for health insurance or employment [9],[15]. Our privacy definition could be used to decide whether to disclose the data set or not due to potential inference issues.

2. Control of data's:

Clearly, details can be manipulated in three ways: adding details to nodes, modifying existing details and removing details from nodes. However, we can broadly classify these three methods into two categories: perturbation and anonymization. Adding and modifying details can both be considered methods of perturbation—that is, introducing various types of "noise" into D to decrease classification accuracies. Removing nodes, however, can be considered an anonymization method [6].

3. Choosing of details Module:

We must now choose which details to remove. Our choice is guided by the following problem statement. This allows us to find the single detail that is the most highly indicative of a class and remove it. Experimentally, we later show that this method of determining which details to remove provides a good method of detail selection [8].

4. Operate Link Information:

The other option for anonymzing social networks is altering links. Unlike details, there are only two methods of altering the link structure: adding or removing links [11].

5. Generalization Module:

To combat inference attacks on privacy, we attempt to provide detail anonymization for social networks. By doing this, we believe that we will be able to reduce the value of an acceptable threshold value that matches the desired utility/privacy tradeoff for a release of data [7].

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Screens:

Fig: Home Page

Fig: Load Data Set

Fig: View Data

Fig: Data Load Separate Tables

Fig: Data Loss Information

Conclusion:

We addressed various issues related to private information leakage in social networks. We show that using both friendship links and details together gives better predictability than details alone. In addition, we explored the effect of removing details and links in preventing sensitive information leakage. In the process, we discovered situations in which collective inferencing does not improve on using a simple local classification method to identify nodes. When we combine the results from the collective inference implications with the individual results, we begin to see that removing details and friendship links together is the best way to reduce classifier accuracy. This is probably infeasible in maintaining the use of social networks. However, we also show that by removing only details, we greatly reduce the accuracy of local classifiers, which give us the maximum accuracy that we were able to achieve through any combination of classifiers. We 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. Similarly, future work could be conducted in identifying key nodes of the graph structure to see if removing or altering these nodes can decrease information leakage.

References:

[1] Facebook Beacon, 2007.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

[2] T. Zeller, "AOL Executive Quits After Posting of Search Data," The New York Times, no. 22, http://www.nytimes.com/2006/08/22/technology/22iht-aol.2558731.html?pagewanted=all&_r=0, Aug. 2006.

[3] 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.

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

[5] 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.

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

[7] 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.

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

[9] 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.

[10] R. Gross, A. Acquisti, and J.H. Heinz, "Information Revelation and Privacy in Online Social Networks," Proc. ACM Workshop Privacy in the Electronic Soc. (WPES '05), pp. 71-80, http://dx.doi.org/10.1145/1102199.1102214, 2005.

[11] H. Jones and J.H. Soltren, "Facebook: Threats to Privacy," technical report, Massachusetts Inst. of Technology, 2005.

[12] P. Sen and L. Getoor, "Link-Based Classification," Technical Report CS-TR-4858, Univ. of Maryland, Feb. 2007.

[13] B. Tasker, P. Abbeel, and K. Daphne, "Discriminative Probabilistic Models for Relational Data," Proc. 18th Ann. Conf. Uncertainty in Artificial Intelligence (UAI '02), pp. 485-492, 2002.

[14] A. Menon and C. Elkan, "Predicting Labels for Dyadic Data," Data Mining and Knowledge Discovery, vol. 21, pp. 327-343, 2010.

[15] E. Zheleva and L. Getoor, "To Join or Not to Join: The Illusion of Privacy in Social Networks with Mixed Public and Private user Profiles," Technical Report CS-TR-4926, Univ. of Maryland, College Park, July 2008.