RESEARCH ARTICLE OPEN ACCESS

Review of Anonymization of Social Networks Concepts And Methods

Priyanka Bhilare*, Prof. Rajesh B. Singh **
*(Department of Computer Engineering, Pune University, India Email: priyanka.bhilare@gmail.com)
** (Department of Computer Engineering, Pune University, India Email: rase69@gmail.com)

ABSTRACT
Nowadays the use of social networks website is growing at phenomenal rate. Social networks involve connections which allow individuals to get connected to their friends and family. The social networking websites like Face book, Twitter, Google+ etc are easily accessible to end users through mobile and any other Internet resources. This open connectivity allows end users to share their sensitive information. If adversary has some background knowledge about an individual, the privacy can be easily leaked. So, the major problem with social networking websites is the risk involved in the privacy and security as they discloses the personal information of the individuals. In this paper, the privacy preservation process is reviewed. In addition to this different privacy preservation methods are presented.

Keywords - Anonymization, Data Mining, Generalization, Privacy Disclosure, Randomization, Security, Sequential Clustering, Social Networks.

1. Introduction

The use of social networks is becoming important in many of the real life applications such as homeland security, psychology, and epidemiology and most importantly for marketing. In the research domains like data mining, sociology, theory communities and sociology, social networking focused more for their analysis and management. Many of the existing works over social networking focused over the study of different properties of social networks as well as finding out effective and efficient methods for analysis [7] [8]. This social networking websites are majorly contenting the user's private information and their personal sensitive relational information. The social networking applications like anonymous web browsing needs the relationship and/or identity anonymity because of confidential, sensitive, stigmatizing nature of end user identities as well as their behaviors [9]. Therefore in recent research works, the privacy preservation in social networks data analysis focused more and became interesting research challenge [10] [11].In actual, the problem of privacy threat in social networking arises whenever the owner of data wants to share or publish important data over social networking for the applications like business related or research oriented. The techniques of social networking privacy preservation are basically used for the privacy protection using masking, modifying and/or generalizing the original data while without compromising more data utility [6]. In this paper we are presenting the detailed review of privacy preservation process in social networks. In addition to this we are taking the review of different types of privacy breaches. A privacy breach is the private information leaking from social networks; this is presented in section II below. After that in section III we are defining the different methodology and methods which comes under the research of privacy preservation in social networks.

II. Review of Social networks Privacy Breaches

When studying privacy, it is important to specify what defines a failure to preserve privacy. A privacy breach occurs when a piece of sensitive information about an individual is disclosed to an adversary, someone whose goal is to compromise privacy. Traditionally, two types of privacy breaches have been studied: identity disclosure and attribute disclosure. We discuss these two types in the context of social networks. We also present two more disclosure types, specific to network data: social link disclosure and affiliation link disclosure.

2.1 Identity Disclosure

Identity disclosure occurs when an adversary is able to determine the mapping from a profile v in the social network to a specific real-world entity p. Before we recognize, disclosure is able to provide a formal definition that may be interested to identify an enemy. Consider three questions. Personal profile v g in a social network and a set of a particular individual Returns is the query definition v. 10.2 survival profile v p, for a particular person maps. And if this person has a profile of v-network g is right or wrong in two separate profiles VI and VJ, and if they are the same person. Refer to return true or false. The anti mapping query correctly and can answer with certainty is a simple way of defining identity disclosure. Until that can be matched to individual features unique characteristics of observed p V in profile with an opponent knows, however, it is difficult to obtain. One way of formalizing identity disclosure for an individual p is to associate a random variable vp which ranges over the profiles in the network. We assume that the adversary has a way of computing the probability of each profile VI belonging to individual p, Pr (ˆvp = VI). In addition, we introduce a dummy profile dummy in the network which serves the purpose of absorbing the probability of individual p not having a profile in the network. We assume that p has exactly one profile, and the true profile of p in V ∪ {dummy} is v. We use the shorthand Prp (VI) = Pr (ˆvp = VI) to denote the probability that VI corresponds to p; Prp provides a mapping Prp: V ∪ {dummy} → R. We leave it open as to how the adversary constructs Prp. Then we can define identity disclosure as follows:

In a set of individual profiles V in a social network G, identity disclosure occurs with confidence t when Prp (v) ≥ t and v = dummy. An alternative definition of identity disclosure considers that the possible values of VI can be ranked according to their probabilities. In a set of individual profiles V in a social network G, identity disclosure occurs with top k confidence when v appears in the top k profiles (or top p% = k 100/|V |), in the list of profiles ranked by Prp from high to low.

2.2 Attribute disclosure

A common assumption in the privacy literature is that there are three types of possibly overlapping sets of personal attributes: Identifying attributes - attributes, such as social security number (SSN), which identify a person uniquely. Quasi-identifying attributes is a combination of attributes which can identify a person uniquely, such as name and address. Sensitive attributes - attributes that users may like to keep hidden from the public, such as politic affiliation and sexual orientation. Attribute disclosure occurs when an adversary is able to determine the value of a sensitive user attribute, one that the user intended to stay private. This attribute can be an attribute of the node itself, the node’s links or the node’s affiliations. Without loss of generality, here we discuss the attributes of the node itself [1] [2]. Again, to make this definition more concrete, we assume that each sensitive attribute v.as for profile v has an associated random variable v.as which ranges over the possible values for v. as. Let the true value of v.as be v.as. We also assume that the adversary can map the set of possible sensitive attribute values to probabilities, Pra (v.as = v.as): v.as → R, for each possible value v.as. Note that this mapping can be different for each node/profile. Now, we can define attribute disclosure as follows: For a profile v with a hidden attribute value v.as = v.as, attribute disclosure occurs with confidence t when Pra (v.as = v.as) ≥ t. Similarly to identity disclosure, there is an alternative definition of attribute disclosure which considers that the possible values of v.As can be ranked according to their probabilities. For a profile v with a hidden attribute value v.as = v.as, attribute disclosure occurs with top-k confidence when appears in the top k values of the list of possible values ranked by their probabilities Pra. Clearly, if an adversary can see the identifying attributes in a social network, then answering the identity mapping query becomes trivial, and identity disclosure with confidence 1 can occur. For example, if a profile contains a SSN, then identifying the re person behind the profile is trivial since there is a one to one mapping between individuals and their social security numbers. Therefore, in order to prevent identity disclosure, the identifying attributes have to be removed from the profiles. Sometimes, a combination of attributes, referred to as quasi-identifying attributes, can lead to identity disclosure. What constitutes quasi-identifying attributes depends on the context. For example, it has been observed that 87% of individuals in the U.S. Census from 1990 can be uniquely identified based on their date of birth, gender and zip code. Another example of quasi-identi years is a combination of a person's name and address [3]. Similarly, matching records from different datasets with quasi-identifying attributes can lead to further privacy breaches. This is known as a linking attack. If the identities of users in one dataset are known and the second dataset does not have the identities but it contains sensitive attributes, then the sensitive attributes of the users from the first dataset can be revealed. For example, matching health insurance records, in which the identifying information is removed, with public voter registration records can reveal sensitive health information about voters. Using this attack, Sweeney was able to identify the medical record of the governor of Massachusetts.

2.3 Social Link Disclosure

Social link disclosure occurs when an adversary is able to hand out about the existence of a sensitive relationship between two users, a relationship that these users would like to remain hidden from the public. Similarly to the previous types of disclosures, we assume that there is a random variable ei,j associated with the link existence between two nodes vi and vj , and an adversary has a model for assigning a probability to ˆei,j , Pr(ˆei,j = true) : ei,j → R. For two profiles VI and VJ, a social link disclosure occurs with confidence t when eV (VI, VJ) Ev and Pr (ˆei, j = true) ≥ t.

Note that since the link existence ei, j has only two possible values, true and false, the top-k definition does not apply to social link disclosure. Examples of sensitive relationships can be found in social networks, communication data, disease data and others. In social network data, based on the friendship relationships of a person and the public preferences of the friends such as political affiliation, it may be possible to infer the personal preferences of the person in question as well [9].

In cell phone communication data, finding that an unknown individual has made phone calls to a cell phone number of a known organization can compromise the identity of the unknown individual.

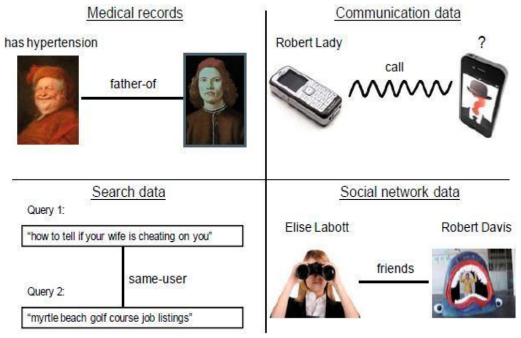


Fig 1. sensitive link example [4]

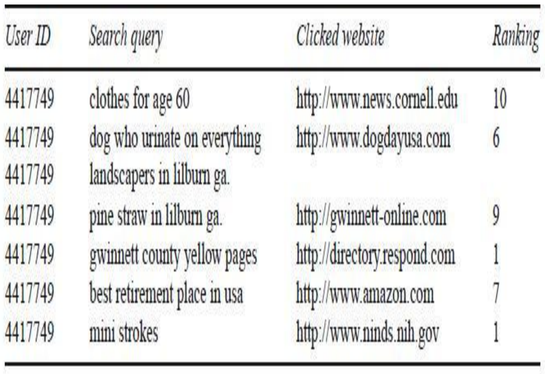
In hereditary disease data, knowing the family relationships between individuals who have been diagnosed with hereditary diseases and ones that have not can help infer the probability of the healthy individuals to develop these diseases. Above figure is showing the summary of these examples.

2.4 Affiliation Link Disclosure

Another type of privacy breach in relational data is affiliation link disclosure whether a person belongs to a particular affiliation group. Whether two users are affiliated with the same group can also be of sensitive nature. Sometimes, affiliation link disclosure can lead to attribute disclosure, social link disclosure, or identity disclosure. Thus, hiding affiliations is a key to preserving the privacy of individuals. As before, we assume that there is a random variable ev,h associated with the existence of an affiliation link between a profile v and a group h, and that an adversary has a way of computing the probability of ˆev,h, Pr(ˆev,h = true) : ev,h → R. For a profile v and an affiliation group h, an affiliation link disclosure occurs with confidence t when he (v, h) Eh and Pr (ˆev, h = true) ≥ t. One type of disclosure can lead to another type. For example, Wondracek et al. show a de-identification attack in which affiliation link disclosure can lead to the identity disclosure of a supposed anonymous Internet user. An adversary starts the attack crawling by a social networking website and collecting information about the online social group memberships of its users. It is assumed that the identities of the social network users are known. According to the collected data, each user who participates in at least one group has a group signature, which is the set of groups he belongs to. Then, the adversary applies a history stealing attack which collects the web browsing history of the target Internet user. By finding the group signatures of social network users which match the browsing history of the Internet user, the adversary is able to find a subset of potential social network users who may be the Internet user. In the last step of the attack, the adversary looks for a match between the id's of the potential users and the browsing history of the target individual, which can lead to de-identification of the Internet user. Another example of affiliation link disclosure leading to identity disclosure is in search data. If we assume that users posing queries to a search engine are the individuals in the social network, and the search queries they pose are the affiliation groups, then disclosing the links between users and queries can help an adversary identify people in the network. Users interact with search engines in an uninhibited way and reveal a lot of personal information in the text of their queries. There was a scandal in 2006 when AOL, an Internet Service provider, released an "anonymized" sample of over half a million users and their queries posed to the AOL search engine. The release was well-intentioned and meant to boost search ranking research by supplementing it with real-world data. Each user was specified by a unique identifier, and each query contained information about the gave away enough personal in for her queries included names of people with the same last name as hers, information about retirement, her location, etc. user identifier, search query, the website the user clicked on, the ranking of that website in the search results, and the timestamp of the query. One of the problems with the released data was that even though it was in a table format (Table1), its entries were not independent of each other. Shortly after the data release, New York Times reporters linked 454 search queries made by the same individual.

TABLE 1

A Snapshot of the Data Released by AOL Here, We Are omitting The Timestamps Included in the Data [4].



User ID	*Search query*	*Clicked website*	*Ranking*
4417749	clothes for age 60	http://www.news.cornell.edu	10
4417749	dog who urinate on everything	http://www.dogdayusa.com	6
4417749	landscapers in lilburn ga.		
4417749	pine straw in lilburn ga.	http://gwinnett-online.com	9
4417749	gwinnett county yellow pages	http://directory.respond.com	1
4417749	best retirement place in usa	http://www.amazon.com	7
4417749	mini strokes	http://www.ninds.nih.gov	1

Affiliation link disclosure can also lead to attribute disclosure, as illustrated in a guilt-by-association attack. This attack assumes that there are groups of users, whose sensitive attribute values are the same, thus recovering the sensitive value of one user and the affiliation of another user to the group can help recover the sensitive value of the second user. This attack was used in the Bit- Torrent file sharing network to discover the downloading habits of users. Communities were detected based on social links, and monitoring only one user in each community was enough to infer the interests of the other people in the community. In this case the sensitive attribute that users would like to keep private is whether they violate copyrights. This attack has also been applied to identifying fraudulent callers in a phone network. Cormode et al. study data anonymization to prevent affiliation link disclosure.

III. Methodology of Social Network Privacy Preservation

3.1 Review of Privacy in Publishing Social Networks

In a social network, nodes usually correspond to individuals or other social entities, and an edge corresponds to the relationship between two entities. Each entity can have a number of attributes, such as age, gender, income, and a unique identifier. The privacy breaches in social networks can be grouped to three categories: The identity disclosure corresponds to the scenario where the identity of an individual who is associated with a node is revealed.

The link disclosure corresponds to the scenario where the sensitive relationship between two individuals is disclosed. The attribute disclosure denotes the sensitive data associated with each node is compromised.Compared with existing anonymization and perturbation techniques of tabular data; it is more challenging to design elective anonymization techniques for social network data because of difficulties in modeling background knowledge and quantifying information loss.

3.2 Related Information

Adversaries usually rely on background knowledge to de-anonymize nodes and learn the link relations between de-anonym zed individuals from the released anonym zed graph. The assumptions of the adversary's background knowledge play a critical role in modelling privacy attacks and developing methods to protect privacy in social network data. Zhou et al. listed several types of background knowledge: attributes of vertices, specific link relationships between some target individuals, vertex degrees, neighborhoods of some target individuals, embedded sub graphs, and graph metrics (e.g., between's, closeness, centrality).

For simple graphs in which nodes are not associated with attributes and links are unlabeled, adversaries only have structural background knowledge in their attacks (e.g., vertex degrees, neighborhoods, embedded sub graphs, graph metrics). For example, Liu and Terzi considered vertex degrees as background knowledge of the adversaries to breach the privacy of target individuals, the authors of paper listed in [5] used neighborhood structural information of some target individuals, the authors of proposed the use of embedded sub graphs, and Ying and Wu exploited the topological similarity/distance to breach the link privacy. For rich graphs in which nodes are associated with various attributes and links may have deferent types of relationships, it is imperative to study the impact on privacy disclosures when adversaries combine attributes and structural information together in their attacks. Re-identification with attribute knowledge

of individuals has been well- studied and resisting techniques have been developed for tabular data. However, applying those techniques directly on network data erases inherent graph structural properties.

3.3 Review of Utility Preservation

An important goal of publishing social network data is to permit useful analysis tasks. Deferent analysis tasks may expect deferent utility properties to be preserved. So far, three types of utility have been considered. Graph topological properties. One of the most important applications of social network data is for analyzing graph properties. To understand and utilize the information in a network, re- searches have developed various measures to indicate the structure and characteristics of the network from deferent perspectives. Properties including degree sequences, shortest connecting paths, and clustering coencients are addressed in various research papers listed in [5]. Graph spectral properties. The spectrum of a graph is usually defined as the set of Eigen values of the graph's adjacency matrix or other derived matrices. The graph spectrum has close relations with many graph characteristics and can provide global measures for some network properties. Spectral properties are adopted to preserve utility of randomized graphs in papers listed in [5]. An aggregate network query calculates the aggregate on some paths or sub graphs satisfying some query conditions. One example is that the average distance from a medical doctor vertex to a teacher vertex in a network. In some papers those are listed in [5], the authors considered the accuracy of answering aggregate net- work queries as the measure of utility preservation. In general, it is very challenging to quantify the information loss in anonym zing social networks. For tabular data is since each tulle is usually assumed to be independent, we can measure the information loss of the anonym zed table using the sum of the information loss of each individual tulle. However, for social network data, the information loss due to the graph structure change should also be taken into account in addition to the information loss associated with node attribute changes.

Zou et al. used the number of modified edges between the original graph and the released one to quantify information loss due to structure change. The rationale of using anonymization cost to measure the information loss is that a lower anonymization cost indicates that fewer changes have been made to the original graph.

3.4 Review of Anonymization Methods

Similar to the design of anonymization methods for tabular data, the design of anonymization methods also need take into account the attacking models and the utility of the data. We categorize the state-of-the-art anonymization methods on simple network data into three categories as follows. This approach modifies graph structure via a sequence of edge deletions and additions such that each node in the modified graph is indistinguishable with at least K¡1 other nodes in terms of some types of structural patterns. This approach modifies graph structure by randomly adding/deleting edges or switching edges. It protects against re-identification in a probabilistic manner.

VI. Conclusions

In this review paper we have presented the study over privacy breaches over the social networking websites in details. In addition to this we introduced the different mechanisms those are directly related to preserving the privacy in social networks. During this review paper our main aim is to present the initial understanding of problem domain and discuss their related methods presented. This paper is prepared by considering our future work in the same research domain. The research and development of privacy-preserving social network analysis is still in its early stage compared with much better studied privacy-preserving data analysis for tabular data. We have many recommendations for the future work, but we focus on further designing of

efficient method for Anonymization of social network by using the robust data mining methods such as sequential clustering.

References

Journal Papers:

[1] A. Acquisti and R. Gross. *Predicting social security numbers from public data.* In PNAS, 2009.

[2] C. C. Aggarwal and P. S. Yu. *Privacy-Preserving Data Mining: Models and Algorithms.* Springer, 2008.

[3] G. Aggarwal, T. Feder, K. Kenthapadi, R. Motwani, R. Panigrahy, D. Thomas, and A. Zhu. *Approximation algorithms for k-anonimity.* JPT, Nov. 2005.

Books:

[4] Elena Zheleva, *chapter 10: privacy in social networks: a survey* Department of Computer Science University of Maryland College Park, MD 20742, USA

[5] Xintao Wu, Xiaowei Ying, Kun Liu, Lei Chen, *a survey of algorithms for privacy-preservation of graphs and social networks* University of North Carolina at Charlotte.

[6] R. Diestel. *graph theory (3rd edition)* volume 173. Springer-Verlag, Heidelberg, 2005.

Theses:

[7] N. Alon and J. Spencer. *The Probabilistic Method*. John Wiley, 1992.

Proceedings Papers:

[8] R. Agrawal, R. Srikant, and D. Thomas. *Privacy preserving olap*. In Proceedings of the 2005 ACM SIGMOD international conference on Management of data (SIG-MOD'05), pages 251{262, New York, NY, USA, 2005. ACM.

[9] 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 Press.

V. Acknowledgment

Thanks to the experts who have contributed towards the development of this material.

[10] Campan and T. M. Truta. *A clustering approach for data and structural anonymity in social networks*. In Proceedings of the 2nd ACM SIGKDD International Workshop on Privacy, Security, and Trust in KDD (PinKDD'08), in Conjunction with KDD'08, Las Vegas, Nevada, USA, 2008.

[11] G. Cormode, D. Srivastava, T. Yu, and Q. Zhang. *Anonymizing bipartite graph data using safe groupings*. In Proceedings of the 34th International Conference on Very Large Databases (VLDB'08). ACM, 2008.