International Journal of Research in Advent Technology, Vol.2, No.10, October 2014
E-ISSN: 2321-9637

Survey on Sensitive Label Privacy Protection on Social Network

Chiranjivi Kariya[1], Sandesha Patil[2], Priyanka Wandile[3]
Department of Computer Engineering, BDCOE, Sewagram, Maharashtra, INDIA
Email: chiranjivi.kariya@gmail.com[1], sandesha_2410@rediffmail,com[2], priyankawandile@gmail.com

Abstract- Sensitive Label and data handling are important issues for social network users. Ideally, access control enforcement should not depend on the social networking provider but should be under the control of the user. a privacy protection scheme that not only prevents the disclosure of identity of users but also the disclosure of selected features in user's profiles also its used to module, a graph where each vertex in the graph is associated with a sensitive label. It makes all requests for private data from third party applications (TPAs) explicit and enables a user to exert fine-grained control over what profiles data can be accessed by them. Users can share their access control configurations for TPAs with their friends who can reuse and rate such configurations. The social networks are modeled as graphs in which users are nodes and features are labels. Labels are denoted either as sensitive or as non-sensitive.

Index Terms- Sensitive Label, TPAs, Privacy Management, Cluster.

1. INTRODUCTION

Sensitive information about users of the social networks should be protected. The challenge is to devise methods to publish social network data in a form that affords utility without compromising privacy. 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 Definition and protection mechanisms leverage structural properties of the graph. This paper is motivated by the recognition of the need for a fine grain and more personalized privacy. Users entrust social networks such as Facebook and LinkedIn with a wealth of personal information such as their age, address, current location or political orientation. They refer to these details and messages as features in the user's profiles. They 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. An individual user can select which features of her profiles she wishes to conceal. The social networks are modeled as graphs in which users are nodes and features are labels. Labels are denoting either as sensitive or as non-sensitive. Figure 1 is a label graph representing a small subset of such a social network. Each node in the graph represents a user, and the edge between two nodes represents the fact that the two persons are friends. Labels annotate 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. (Labels are in red italic in Figure 1). The privacy issue arises from the disclosure of sensitive labels. One might suggest that such labels should be simply deleted.

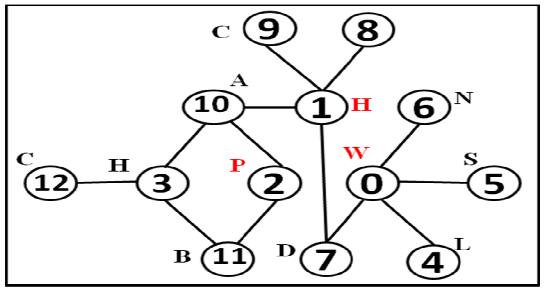

Figure 1. Example of the labeled graph representing a social network.

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. They consider such threats as neighborhood attack, in which an adversary find out sensitive information based on prior knowledge of the number of neighbors of a target node and the labels of these neighbors. In the 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). They 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 an adversary cannot safely infer the identity and sensitive labels of users. They consider the case in which the adversary possesses structural knowledge and label information. The algorithms that, they propose transform the original graph into a graph in which any node with a sensitive label is indistinguishable from at least 1 other node. (The probability to infer that any node has Sensitive nodes) is no larger than one for this purpose they design diversity like model, where they 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. In view of the tradeoff between data privacy and utility [16]. They evaluate empirically the extent to which the algorithms preserve the original graph's structure and properties such as density, degree distribution and clustering coefficient. They 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. PROPOSED SYSTEM

In order to concern with social network privacy and data hiding is the major problem. According to existing system, currently available module is profiling and friend request. Profiling consist user (node) private/public data and friend request contain Third party which they want to interact.in the proposed system, they explore the two new module name as, privacy option and new graph positioning. In real world there were many privacy option as , only me ,friends of friends, private/public but, in order to used these option still there is problem to often tagged the information and this is obviously violate privacy and also experienced more revelation. Here they are providing one more facility i.e. make a group within group and finely exchange of data can be possible. Whenever to give privacy in group it will become more secure and also help to make sure to upload text or may called information were use by know third party. It is easy to plot graph in group of the friend relationship.

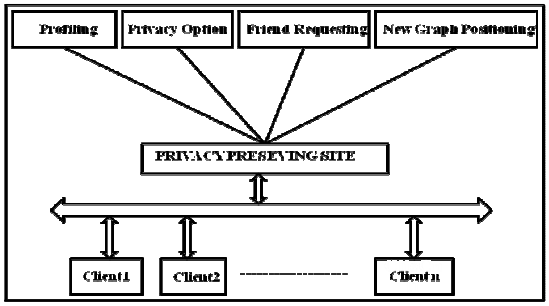

Figure 1: Privacy preserving network

The social networks are modelled as graphs in which nodes and features are labels. Labels are denoted either as sensitive or as non-sensitive.

2.1. Problem Definition

They model a network as G (V; E; Ls; L;Γ**),** where V is a set of nodes, E is s set of edges, Ls is a set of sensitive labels, and L is a set of non-sensitive labels. Γ Maps nodes to their labels,Γ :$V \rightarrow L^s \cup L$. Then they propose a privacy model, ℓ-sensitive-label-diversity; in this model, they treat node labels both as part of an adversary's background knowledge, and as sensitive information that has to be protected. These concepts are clarified by the following definitions:

1. Definition 1. The neighbourhood information of node v comprises the degree of v and the labels of vs. neighbours.

2 Definition 2. (*ℓ`-Sensitive-label-diversity*) For each node v that associates with a Sensitive label, there must be at least ℓ - 1 Other nodes with the same neighbourhood Information, but attached with different Sensitive labels.

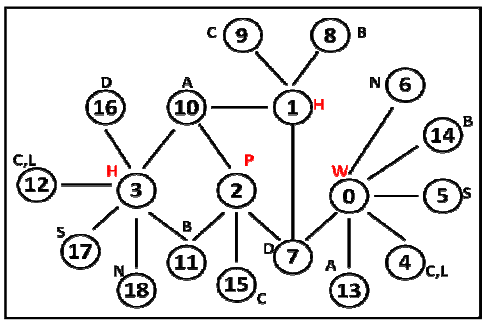

Figure 2 .Privacy-attaining network examples.

In Example 1, nodes 0, 1, 2, and 3 have sensitive labels. The neighbourhood information of node 0, includes its degree, which is 4, and the labels on nodes 4, 5, 6, and 7, which are L, S, N, and D,

respectively. For node 2, the neighbourhood information includes degree 3 and the labels on nodes 7, 10, and 11, which are D, A, and B. The graph in Figure 2 satisfies sensitive label-diversity that is because, in this graph, nodes 0 and 3 are indistinguishable, having six neighbours with label A, B,{ C,L}, D, S, N separately; likewise, nodes 1 and 2 are indistinguishable, as they both have four neighbours with labels A, B, C, D separately.

2.2. Algorithm

They are grouping nodes as similar neighbourhood information as possible so that they can change as few labels as possible and add as few noisy nodes as possible. In the first run, two nodes with the maximum similarity of their neighbourhood labels are grouped together. Their neighbour labels are modified to be the same immediately so that nodes in one group always have the same neighbour labels. For two nodes, v1 with neighbourhood label set (LSv1), and v2 with neighbourhood label set (LSv2), we calculate neighbourhood label similarity (NLS) as follows:

$$NLS(v_1, v_2) = \frac{|LS_{v_1} \cap LS_{v_2}}{|LS_{v_1} \cup LS_{v_2}} \quad \text{.....(1)}$$

Larger value indicates larger similarity of the two neighbourhoods. Then nodes having the maximum similarity with any node in the group are clustered into the group till the group has ℓ nodes with different sensitive labels. Thereafter, the algorithm proceeds to create the next group. If fewer than ℓ nodes are left after the last group's formation, these remainder nodes are clustered into existing groups according to the similarities between nodes and groups. After having formed these groups, they need to ensure that each group's members are indistinguishable in terms of neighbourhood information. Thus, neighbourhood labels are modified after every grouping operation, so that labels of Nodes can be accordingly updated immediately for the next grouping operation. This modification process ensures that all nodes in a group have the same neighbourhood information.

The objective is achieved by a series of modification Operations. To modify graph with as low information loss as possible, they devise three modification operations: label union, edge insertion and noise node addition.

Label union and edge insertion among nearby nodes are preferred to node addition, as they incur less alteration to the overall graph structure. If there are nodes in a group still having different neighbourhood information, noise nodes with non-sensitive labels are added into the graph so as to render the nodes in group indistinguishable in terms of their neighbour's labels.

They consider the unification of two nodes' neighbourhood labels as an example. One node may need a noisy node to be added as its immediate neighbour since it does not have a neighbour with certain label that the other node has; such a label on the other node may not be modifiable, as it's already connected to another sensitive node.

3. LITERATURE REVIEW

Haying Shen, Ze Li, Yuhua Lin was implemented the concept of SocialTube: P2P-assisted Video Sharing in Online Social Networks worked by Haiying Shen, Ze Li, Yuhua Lin. i,e, client/Server architecture deployed by Current video sharing system in Social network most a large amount of Resource for service provider and lack of scalability. Hence most of the video views are drive by Social relationship and rest of drive by Interest and viewer of the same video tend to reside in the same location. Based on their observation, they proposed SocialTube a system that was explores a Social relationship, SocialTube can provide a low video Start-up delay and low server Traffic. in this topic SN – Based Chunk Peftching Algorithm was implemented.[2]

Preventing Private Information Inference Attacks on Social Networks was proposed by Raymond Heatherly, Murat Kantarcioglu, Bhavani Thuraisingham. That was the first paper that discussed the problem of sanitizing a social network to prevent inference of social network data and then examine the effectiveness of those approaches on a real-world dataset. In order to protect privacy, i.e., deleting some information from a user's profile and removing links between friends. They had presented a modification of the Naıve Bayes classification algorithm that was use details about a node, and link structure, to predict private details. The network consists of only nodes and edges. Trait details are not included. The goal of the attacker is to simply identify people. [15]

In 2013 author Lan Zhang, Xiang-Yang Li ternational was explored the concept of Distributed Computing Systems on Privacy Preserving Friending in Social Networks by. Their mechanisms establish a secure communication channel between the initiator and matching users at the time when the matching user is found. This method was encryption based. The main idea of our mechanism is to use the request profile as a key to encrypt a message. Only a matching user, who shares the secret, can decrypt the message with his/her profile efficiently.

The concept of Fairness-aware and Privacy-Preserving Friend Matching Protocol in Mobile Social Networks was implemented by Haojin Zhu, Suguo Du, Muyuan Li and Zhaoyu Gao. In that paper, they

proposed their privacy-preserving and fairness-aware interest and profile matching protocol, which allows one party to match its interest with the profile of another, without revealing its real interest and profile and vice versa. The protocol proposed in this paper was based on Paillier's homomorphic encryption

Outsourcing Privacy-Preserving Social Networks to a Cloud was proposed by Guojun Wang, Qin Liu, Feng Li, Shuhui Yang and Jie Wu. The main design goal of their work was to reduce the probability of a social actor being re-identified while publishing social networks to a cloud In this paper, they were identify a novel type of privacy attack, termed 1 neighbourhood attack, where an attacker is assumed to know the degrees of they consider a system that consists of a publisher, a cloud service provider. [11]

In 2013, Hongxin Hu, Hongxin Hu, Ziming Zhao was prosed the theory on Game Theoretic Analysis of Multiparty Access Control in Online Social Networks. They were explored that a multiparty Access Control (MPAC) model was recently proposed, including a systematic approach to identify and resolve privacy conflicts for collaborative data sharing in OSNs. In this paper, They take another step to further study the problem of analyzing the strategic behaviour of rational controllers in multiparty access control, where each controller aims to maximize her/his own benefit by adjusting her/his privacy setting in collaborative data sharing in OSNs.

International Conference on Pervasive Computing and Communication Workshop 2010 on topic Relationship-based Access Control for Online Social Networks: Beyond User-To-User Relationships was presented by Yuan Cheng, Jaehong Park and Ravi Sandhu to ensure that U2U relationship. In this paper, they developed a relationship-based access control model for OSNs that incorporates not only U2U relationships but also user-to-resource (U2R) and resource-toresource (R2R) relationships. Furthermore, while most access control proposals for OSNs only focus on controlling users' normal usage activities, their model also captures controls on users' administrative activities. Authorization policies are defined in terms of patterns of relationship paths on social graph and the hopcount limits of this path. [7].

Aaditeshwar Seth was prosed the on Design of a Social Network Based Recommender System for Participatory Media Conten. In that paper, they presented an overview of our work in sociological theory and user modelling outlines the system design for a recommender system that makes use of this work, describe some open problems, and focus on one component of the System that is strongly grounded in social network theory.

NOYB: Privacy in Online Social Networks was proposed by Saikat Guha, Kevin Tang, Paul Francis they proposed the system like NOYB short for none of your business was based on the observation that some online services notably social networking websites can operate on "fake"data. The solution was that user data was first encrypted and the cipher text encoded to look like legitimate data. The online services can operate on the ciphered data, however only authorized users can decode and decrypt the result. A simplistic approach would be to encrypt each atom and share the key with other users authorized to view that atom. While such a scheme does not reveal any users information to the online services. [5].

Supporting Privacy Protection in Personalized Web Search proposed by Lidan Shou, He Bai, Ke Chen, and Gan Chen and proposed system i,e, Personalized web search (PWS) has demonstrated its effectiveness in improving the quality of various search services on the Internet. They propose a PWS framework called UPS that can adaptively generalize profiles by queries while respecting user specified privacy requirements. They also provide an online prediction mechanism for deciding whether personalizing a query is beneficial [6].

In 2005, Mr. Ralph Gross, Mr. H. John Heinz they was proposed the concept of Information Revelation and Privacy in Online Social Networks. That paper was based on the information they provide online, users expose themselves to various physical and cyber risks, and make it extremely easy for third parties to create digital dossiers of their behavior. These risks are not unique to the Facebook. However, the Facebook's public linkages between an individual profile and the real identity of its owner, and the Facebook's perceived connection to a physical and ostensibly bounded community (the campus), make Facebook users a particularly interesting population for our research. [4].

Mr. A.Stalin Irudhaya Raj, Ms. N.Radhi was presented paper on Securing Sensitive Information in Social Network Data Anonymization to secure sensitive Information in social network data anonymization using k-degree-l-diversity anonymity model. The disadvantages of the existing system were that it simply removing the identifiers in social networks does not guarantee privacy. In this paper k-degree anonymity with l-diversity to prevent not only the reidentification of individual nodes but also the revelation of a sensitive attribute associated with each node. [3].

4. CONCLUSION AND RESULT

From above survey paper, they were concluding that, it is must to hide the sensitive data from thirty party applications (TPAs). 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 also our approach in maintaining critical graph properties while providing a comprehensible privacy guarantee.

REFERENCE

[1] Yi Song, Panagiotis Karras_, Qian Xiao, and St_ephane Bressan, IEEE transactions on knowledge and data engineering vol:25 no:3 year 2013cations-Accidentally-leaking access-third parties.

[2] Haiying Shen, Ze Li, Yuhua Lin IEEE Knowledge and data engineering 2009. Kanonymization with SocialTube: P2P-assisted Video Sharing in

[3] Mr. A.Stalin Irudhaya Raj, Ms. N.Radhi . Securing Sensitive Information in Social Network Data Anonymization ENISA Position Paper N.1; 2007. IEEE. W2SP 2008. Web 2.0 security and privacy: 2008.

[4] R. Ralph Gross, Mr. H. John Heinz Information Revelation and Privacy in Online Social Networks. of ACM CCS'12, pp.617-627, 2012.

[5] Saikat Guha, Kevin Tang, Paul Francis NOYB: Privacy in Online Social Network Frontiers,pages 1{14, 2010}.

[6] LIDAN SHOU, HE BAI, KE CHEN, AND GAN CHEN. Supporting Privacy Protection in Personalized Web Search IEEE International Conference on Privacy, Security, Risk and Trust, 2011 IEEE International Conference on, 2011

[7] Yuan Cheng, Jaehong Park and Ravi Sandhu Relationship-based Access Control for Online Social Networks: Beyond User-To-User

[8] QI, Y., AND ATALLAH, M. Efficient privacy-preserving k- nearest neighbour search. In IEEE ICDCS, 2008, pp. 311–319.

[9] B. Li, M. Ma, Z. Jin, and D. Zhao. Investigation of a large-scale P2P VoD overlay network by measurements. Peer-to-Peer Networking and Applications, 5(4):398–411, 2012.

[10] CHASE, M. Multi-authority attribute based encryption. Theory of Cryptography, 2010, pp. 515–534.

[11] Guojun Wang, Qin Liu, Feng Li, Shuhui Yang and Jie Wu., "Outsourcing Privacy-Preserving Social Networks to a Cloud" ICWSM, 2008.

[12] DE CRISTOFARO, E., AND TSUDIK, G. Practical private set intersection protocols with linear Complexity. Financial Cryptography and Data Security, 2010, pp. 143–159.

[13] STAJANO, F., AND ANDERSON, R. The resurrecting duckling: Security issues for ad-hoc wireless networks. In Security Protocols, 2011 pp. 172–182.

[14] DE CRISTOFARO, E., AND TSUDIK, G. Practical private set intersection protocols with linear complexity. Financial Cryptography and Data Security, 2010, pp. 143–159.

[15] Raymond Heatherly, Murat Kantarcioglu, Bhavani Thuraisingham Preventing Private Information Inference Attacks on Social Networks Information Security Practice and Experience, 2008, pp. 347–360.

[16] A. Seth and J. Zhang, "A Social Network Based Approach to Personalized Recommendation of Participatory Media Content," ICWSM, 2008