International Journal of Trend in Scientific Research and Development (IJTSRD)
International Open Access Journal
ISSN No: 2456 - 6470 | www.ijtsrd.com | Volume - 2 | Issue – 3

Attribute Couplet Attacks and Seclusion Protection in Social Networks

S. Archana
B.E (IV-CSE), Ponnaiyah Ramajayam College of Engineering and Technology, Thanjavur, Tamil Nadu, India

A. Sowndarya
B.E (IV-CSE), Ponnaiyah Ramajayam College of Engineering and Technology, Thanjavur, Tamil Nadu, India

R. Banumathi
Assistant Professor, Ponnaiyah Ramajayam College of Engineering and Technology, Thanjavur, Tamil Nadu, India

ABSTRACT

The emerging of social networks, e.g., Face book, Twitter, and Instagram, has eventually changed the way in which we live. Social networks are acquiring and storing a significant amount of profile information and daily activities of over billions of active users. We describe the system which is avoiding the couplet (pair) to restrict another website. We propose the concept k(0) which are avoid the interlink between the websites. In existing they used the concept of k-couplet anonymity which are multiple attribute social network to realize the k-couplet anonymity. Design an approximate algorithm for multiple-attribute social networks to realize the k-couplet anonymity. To deal with the problem of privacy leakage, a number of attack models and corresponding privacy preserving solutions have been proposed recently. A common approach is to anonymize the identities of the users when publishing the data sets.

Keywords: *social networks, k-couplet anonymity, data sets*

INTRODUCTION

Human's activities on social networks are booming with the fast popularity of smart mobile devices (e.g., smart phones, tablets) and pervasive availability of high speed networks (e.g., Wifi and 4G). Social networks including Face book, Twitter, Instagram provide prolific services for the users meanwhile maintaining millions or even billions of users' profile information and daily routines. Datasets drawn from social networks are attracting significant attentions from different research communities and have been studied extensively in the literature. Releasin the datasets will Fosterther search on social networks and is possible to bring new services for the users. However, one major concern on publishing these datasets is the potential privacy leakage of the individuals involved in the datasets.

The sensitive information of the individuals is exposed under many different types of privacy attacks, including structural attacks, neighborhood attacks, mutual friends attacks, etc.,. The privacy leakage leads to unprecedented social and economic losses. Many researchers have been proposed recently to deal with the above privacy attacks on social networks. The common principle behind these.

Approaches are to guarantee anonymity for the individuals so that the privacy can be preserved. Social networks can be represented as directed or undirected graphs and we only consider the undirected graph Data set drawn from the social networks are restricted This commentary discusses the complex relationship between social networks and the EU Data Protection Directive After a concise introduction to the general privacy impact of social networks, it discusses how the Directive applies to users and operators of social networks and social network applications. The fundamental objectives of any decision problem should define why the decision maker is interested in that decision. However, listing a complete set of the fundamental objectives for a decision is not a simple task. It requires creativity,

time, some hard thinking, and the recognition that it is important. This chapter offers many suggestions to help do the task well and provides criteria to appraise the quality of the resulting set of fundamental objectives.

DESIGN

WEB SERVICES

Web Services module will use the interfaces defined for the example Stateless adapter module prepared in creating an example Stateless adapter module. The Web Services module will have the following properties: Package: com.acompany.wespa.mysctype Interface used by the client, acting on the Web Services module: My Service Capability Interface used by the Web Services module, acting on the client: My Service Capability Listener Method implemented by the Web Services module for application-initiated requests, defined in the My Service Capability interface:

PROTECT IDENTITIES

Secure Identities enable security solutions for smart factories. Secure Identities. Enabling and supporting. Modules (TPMs) offer a standardized solution for efficiently implementing Secure Identities. Using Trusted Platform Modules as standardized trust anchors.

USERS

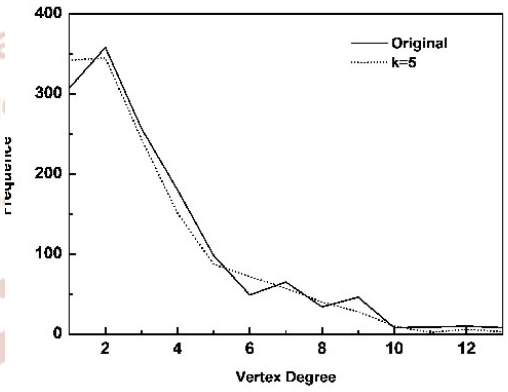
When users access the system through Portal Direct Entry, they are considered guests until they log in. The Login Module is a portal module that allows users to type a user name and password to log in. This module can be placed on any module tab to allow users to log in to the system.

K-COUPLET ANONYMITY

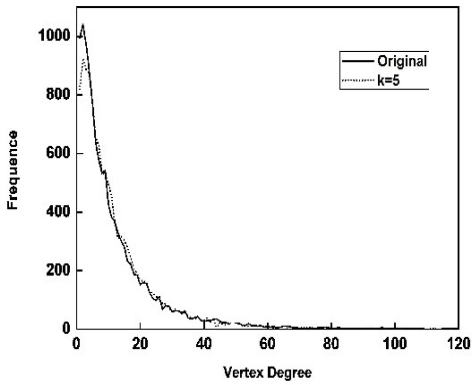
K-anonymity*:* a model for protecting privacy. International Journal on Uncertainty, provided in this paper includes a formal protection model named k-anonymity and a set of accompanying policies

IMPLEMENTATION

Here the proposed system after the implementation of system such as finger print, palm access, iris access, signature and login process are carried out for increasing the authentication.fig shows the results of the proposed system.



(a)



And the proposed method is tested with two ratio such us database template and the captured template. It should give the detailed difference between the

quality, psnrlevel, regions and number of segments in the finger print.

RELATED WORK

Clustering with Multi-Layer Graphs: A Spectral Perspective (Dong. X, Frossard .P,Vandergheynst.P)year 2012 Observational data usually comes with a multimodal nature, which means that it can be naturally represented by a multi-layer graph whose layers share the same set of vertices(users) with different edges (pair wise relationships).

We address the problem of combining different layers of the multi-layer graph for improved clustering of the vertices compared to using layers independently. We propose two novel methods, which are based on joint matrix factorization and graph regularization framework respectively, to efficiently combine the spectrum of the multiple graph layers, namely the eigenvectors of the graph Laplacian matrices. In each case, the result in combination, which we call a "joint spectrum" of multiple graphs, is used for clustering the vertices. We evaluate our approaches by simulations with several real world social network datasets. Results demonstrate the superior or competitive performance of the proposed methods over state-of-the-art technique and common baseline methods, such as co-regularization and summation of information from individual graphs. Address the problem of combining different layers of the multi-layer graph for improved clustering of the vertices compared to using layers independently. propose two novel methods, which are based on joint matrix factorization and graph regularization framework respectively, to efficiently combine the spectrum of the multiple graph layers, namely the eigenvectors of the graph Laplacian matrices.

Privacy Preserving Techniques in Social Networks Data Publishing-A Review (Singh.A,Bansal.D,Sofat.S) year 2014

Development of online social networks and publication of social network data has led to the risk of leakage of confidential information of individuals. This requires the preservation of privacy before such network data is published by service providers. Privacy in online social networks data has been of utmost concern in recent years. Hence, the research in this field is still in its early years. Several published academic studies have proposed solutions for providing privacy of tabular micro-data. But those techniques cannot be straight forwardly applied to social network data as social network is a complex graphical structure of vertices and edges. Techniques like k-anonymity, its variants, L-diversity have been applied to social network data. Integrated technique of K-anonymity & L-diversity has also been developed to secure privacy of social network data in a better way.

The research in this field is still in its early years. Several published academic studies have proposed solutions for providing privacy of tabular micro-data. But those techniques cannot be straight forwardly applied to social network data as social network is a complex graphical structure of vertices and edges.

Resisting Structural Re-identification in Anonymized Social Networks (Hay.M, Miklau .G,Jensen.D,Towsley.D) year 2008

We identify privacy risk associated with releasing network data Sets and provide an algorithm that mitigates those risks. A network consists of entities connected by links representing relations such as friendship, communication, or shared activity. Maintaining privacy when publishing networked data is uniquely challenging because an individual's network context can be used to identify them even if other identifying information is removed. We quantify the privacy risks associated with three classes of attacks on the privacy of individual sin networks, based on the knowledge used by the adversary. We show that the risks of these attacks vary greatly based on network structure and size. We propose a novel approach to anonym zing network data that models aggregate network structure and then allows samples to be drawn from that model. The approach guarantees anonymity for network entities while preserving the ability to estimate a wide variety of network measures with relatively little bias. Propose a novel approach to anonymizing network data that models aggregate network structure and then allows samples to be drawn from that model. The approach guarantees anonymity for network entities while preserving the ability to estimate a wide variety of network measures with relatively little bias.

Protecting sensitive labels in social network data anonymi-zation (Navnath.B,Bagal.S) year 2014 Privacy is one of the major concerns when publishing or sharing social network data for social science research and business analysis. Recently, researchers have developed privacy models similar to k-anonymity to prevent node re identification through structure information. However, even when these privacy models are enforced, an attacker may still be

able to infer one's private information if a group of nodes largely share the same sensitive labels (i.e., attributes). In other words, the label-node relationship is not well protected by pure structure anonymization methods. Furthermore, existing approaches, which rely on edge editing or node clustering, may significantly alter key graph properties. We define a k-degree-l-diversity anonymity model that considers the protection of structural information as well as sensitive labels of individuals. We further propose a novel anonymization methodology based on adding noise nodes. We develop a new algorithm by adding noise nodes into the original graph with the consideration of introducing the least distortion to graph properties. Most importantly, we provide a rigorous analysis of the theoretical bounds on the number of noise nodes added and their impacts on an important graph property. We conduct extensive experiments to evaluate the effectiveness of the proposed technique. Propose a scheme namely K-degree-L-diversity model useful for preserving social network data. Our anonymization methodology based on addition of noise nodes into the original social graph which reduces error rate and performs better results.

Privacy Leakage of Location Sharing in Mobile Social Networks: Attacks and Defense(Li.H,Zhu.H,Du.S)

Along with the popularity of mobile social networks (MSNs) is the increasing danger of privacy breaches due to user location exposures. In this work, we take an initial step towards quantifying location privacy leakage from MSNs by matching the users' shared locations with their real mobility traces. We conduct a three-week real-world experiment with 30 participants and discover that both direct location sharing (e.g., Weibo or Renren) and indirect location sharing (e.g., Wechat or Skout) can reveal a small percentage of users' real points of interests (POIs). We further propose a novel attack to allow an external adversary to infer the demographics (e.g., age, gender, education) after observing users' exposed location profiles. We implement such attack in a large real-world dataset involving 22,843 mobile users. The experimental results show that the attacker can effectively predict demographic attributes about users with some shared locations.

To resist such attacks, we propose SmartMask, a context-based system-level privacy protection solution, designed to automatically learn users' privacy preferences under different contexts and provide a transparent privacy control for MSN users. The effectiveness and efficiency of SmartMask have been well validated by extensive experiments.

CONCLUSION

We consider the privacy preserving problem in social networks. Considering the special structure of social networks, we raise a new privacy attack risk termed as attribute couplet attack which utilizes the couplets of attributes to infer the identities in an anonymized social networks. To deal with this attack risk, we propose the concept of k-couplet anonymity and design the corresponding anonymization algorithms. According to the evaluations on multiple public datasets, our proposed algorithms are able to preserve the privacy and utility of the social network dataset effectively under the attribute couplet attacks.

FUTURE ENHANCEMENT

To improve the performance of the KDC, the developers of HDFS chose to use a number of tokens for communication secured with an RPC digest scheme. The Hadoop security design makes use of Delegation Tokens, Job Tokens, and Block Access Tokens. Each of these tokens is similar in structure and based on HMAC-SHA1. Delegation Tokens are used for clients to communicate with the Name Node in order to gain access to HDFS data; while Block Access Tokens are used to secure communication between the Name Node and Data Nodes and to enforce HDFS file system permissions. On the other hand, the Job Token is used to secure communication between the Map Reduce engine Task Tracker and individual tasks. Note that the RPC digest scheme uses symmetric encryption and depending upon the token type, the shared key may be distributed to hundreds or even thousands of hosts.

REFERENCES

1) Cai.Z Nov. 2016, Guan.X Nov. 2016, He.Z Nov. 2016, and Li.y Nov. 2016, ''Collective data-sanitization for preventing sensitive information inference attacks in social networks,'' IEEE Trans. Depend. Sec. Comput., Nov. 2016.

2) Cai.Z Mar2017, Li.Y Mar2017,Wang.C Mar2017,Yu.J Mar2017,Zheng.X Mar2017, and ''Follow but no track: Privacy preserved profile publishing in cyber-physical social systems,'' IEEE Internet Things J., Mar. 2017.

3) Chen.L(2009),andÖzsu.M.T(2009),Zou.L (2009),''Kautomorphism:A general frame work

for privacy preserving network publication,'' Proc. VLDB Endowment, vol. 2, no. 1, pp. 946–957, 2009.

4) Chen,M. S 2011,Tai .C. H 2011, Yang.D. N 2011, and Yu.P.S 2011 ''Privacy-preserving social network publication against friendship attacks,'' inProc. 17th ACMSIGKDD Int. Conf.Knowl. Discovery DataMining, 2011 ,pp.1262–1270

5) Dong.X,(Nov2012),Frossard.P(Nov2012), Nefedov.N,(Nov2012)Vandergheynst.P,(Nov2012) and ''Clusteringwith multi-layer graphs: A spectral perspective,'' IEEE Trans. Signal Process., vol. 60, no. 11, pp. 5820–5831,.

6) Fu.Y 2013, Kong.X 2013, Philip.S.Y 2013,Sun.C 2013, ,and, ''Privacy preserving social network publication against mutual friend attack,inProc.13thInt.Conf. Data Ming Mining Workshops (ICDMW), 2013, pp. 883–890.