ASIAN JOURNAL OF PHARMACEUTICAL AND CLINICAL RESEARCH

INNOVARE ACADEMIC SCIENCES
Knowledge to Innovation

Special Issue (April)

Online - 2455-3891
Print - 0974-2441

Full Proceeding Paper

A SURVEY ON PRIVACY-PRESERVING TECHNIQUES FOR SOCIAL NETWORK DATA

SHARATH KUMAR J, MAHESWARI N

Department of Computer Science and Engineering, VIT University, Chennai, Tamil Nadu, India. Email:asha.s@vit.ac.in

Received: 23 January 2017, Revised and Accepted: 03 March 2017

ABSTRACT

In this era of 20th century, online social networks such as Facebook and Twitter play a very important role in everyone's life. Social network data, regarding any individual organization, can be published online at any time, in which there is a risk of information leakage of anyone's personal data. Hence, preserving the privacy of individual organizations and companies is needed before data are published online. Therefore, this research was carried out in this area for many years and it is still going on. There have been various existing techniques that provide the solutions for preserving privacy to tabular data called as relational data and also social network data represented in graphs. Different techniques exist for tabular data but we cannot apply directly to the structured complex graph data, which consist of vertices represented as individuals and edges represented as some kind of connection or relationship between the nodes. Various techniques such as K-anonymity, L-diversity, and T-closeness exist to provide privacy to nodes, and techniques such as edge perturbation and edge randomization are available to provide privacy to edges in social network graphs. Development of new techniques by integration into the exiting techniques such as K-anonymity, edge perturbation, edge randomization, and L-diversity to provide more privacy to relational data and social network data is ongoing in the best possible manner.

Keywords: Privacy models, K-anonymity, L-diversity, Social networks, Graph perturbation, Randomization.

DOI: http://dx.doi.org/10.22159/ajpcr.2017.v10s1.19587

INTRODUCTION

The Internet in this age has changed the way of communication between people within society. Communication among people takes place through telephone in the earlier days, but now, various online social network sites are available for enabling the communication by content exchange in the form of links, texts, and multimedia posts to share everything among various people [1]. Social network sites such as Twitter, Facebook, Orkut, and LinkedIn generate tremendous amount of data, as more people share their thoughts, feelings, be online to get updates, and share their day-to-day activities. These data are called the social data and are best represented in nodes and edges. These data are collected from multiple users; sources are dynamic in nature and should be updated continuously. The social data which are collected can be used for research purpose or can be used by the data service provider by giving these data to the various other companies, organizations, or other parties such as advertising partners when users agree to the terms and conditions of that service provider. People's data contain very sensitive and valuable information; advertising companies can take advantage of these data and target a social network user.

Social network analysis is used in various fields such as biology, anthropology, sociology, geography, criminology, and information sciences. Researchers from various different fields use these data to improve security of sensitive information which points to the identity of an individual. It is up to the owner of the data whether he/she wants to publish the entire data online or keep some secret data and publish limited information only. There also exist various owners who are sharing the data to the third party applications for data processing, and privacy breach can also occur due to this [2]. At present, we can describe that social network analysis is a technique for investigating the social structures consisting of vertices and edges. A vertex is also called node which represents peoples, groups, organizations, and knowledge entities. The links which connect these nodes are called edges and can hold information which can be sensitive or non-sensitive data [3]. Sharing of these data online may lead to privacy breach. An individual's privacy is defined as "the right of the individual to whom he/she is communicating, what he/she is sharing, and under what circumstances" [4]. Breaching of privacy occurs when information is leaked without getting the permission of individuals, company, and organization. Therefore, the privacy preservation of individuals or any organization before publishing the data is a very important research area. The research involves identifying what type of privacy is required and the data to be classified as sensitive, non-sensitive, or quasi-identifiers (which points to sensitive data) for achieving that privacy.

The paper is designed as follows: Segment 2 defines the different categories of privacy breach which have been identified so far followed by the different challenges in preserving privacy in social network data described in segment 3. Segment 4 gives the description of the existing privacy-preserving techniques for tabular micro-data while segment 5 defines the privacy-preserving techniques for social network data. Segment 6 gives the directions to the new researchers and finally segment 7 concludes the review.

CLASSIFICATION OF PRIVACY BREACH

Privacy breaches can be termed as information leakage leading to identify some sensitive information in social networks and can be classified into three different types [5].

Identity disclosure

This disclosure occurs when a particular individual or user behind a record is disclosed. This type of breach leads to leakage of information of a user and type of relationship he/she shares with any other individuals. Naive anonymization is a technique that removes the entire personal identifying information or replaces it with any other pseudo-random information. This is usually present as nodes in the social network.

Sensitive link disclosure

The links between nodes carry relationship information or strength of a relationship and this disclosure can occur when any edge connection or relation between two entities is leaked. There are social media which gather these types of leaks and publish these data and make money from this information.

Sensitive attributes' disclosure

This disclosure occurs when an adversary gains someone's personal, sensitive, and confidential individual attribute. Sometimes, it is represented as labels in a network. This information contains clusters of data under a common title and here the edges in the network will be sensitive. A shortest edge value indicates highest affinity of an attribute for an individual.

The above-specified breaches provide severe threats such as blackmailing, robbery to the individual because individual expects that service providers provides privacy in the end. Other than that, it also damages the reputation and the image of an individual. Various types of examples are available in which individual information is disclosed accidentally and due to that organization or company has to become more precautious while releasing the social network data [6]. Therefore, some criteria should be defined to address the above-mentioned issues. Data collected from social networking sites have to be released to third parties in such a way that privacy of the users must be ensured. Various techniques such as perturbation and anonymization are available that provide privacy before releasing or publishing data to the third parties. Quasi-identifiers are again a major concern where privacy techniques are required to handle indirect identification. The privacy preservation to social network data is different from that of tabular micro-table data and difficult which is detailed in the upcoming segment.

MAJOR CONCERNS ASSOCIATED IN PRESERVING PRIVACY FOR SOCIAL NETWORK DATA PUBLISHING

Privacy for social network data can be ensured in a different way than that of relational tabular micro-data because [6]:

- It is very difficult to present the background knowledge of an individual or others in social network data when compared to tabular relational data. Relational data can be represented easily in tables and users can be identified easily by connecting the quasi-identifiers from multiple resources in social network such as labels of vertices, also neighborhood graphs can be used to identify individuals.
- Certain metrics exit in relational table such as information loss which counts the amount of distortion. In tabular micro-data, information loss of complete data can be measured easily by adding all information loss in the individual's records. Social network is a graph structure represented by nodes and edges, and when very complex network builds, it is very difficult to measure the information loss and we have to divide it into subgraphs to compare the various graph structures to identify information loss. There exist techniques such as anonymization and randomization in which social networks have same number of nodes and vertices before performing operation and after operation, and different metrics exist here are between-ness, connectivity, and diameter, but they can be measured in different ways also.
- Relational data can be anonymized using various techniques such as divide and conquer approach, but in social networks which consist of individuals as nodes and relationships as edges, it is difficult because, before performing any operation on nodes and edges, we have to analyze whether it affects other nodes and edges after performing operation.

Hence, from the above-mentioned facts, one can conclude that methods that have been developed for relational tabular micro-data cannot be applied directly to social network data, as in social networks, nodes and edges are linked together. Any other unknown person can misuse the information of others in networks. Therefore, some techniques should be developed which can give the guarantee of privacy of data in social network data publishing. Also, it is useful in providing information without sensitive data identification.

PRIVACY-PRESERVING TECHNIQUES FOR RELATIONAL DATA

Various researchers have done a lot of work for privacy preserving in relational data. Techniques such as K-anonymity [7,14], L-diversity [9], and T-closeness [10] have been explained which had shown very extraordinary results in anonymization. Fig. 1 provides the brief overview of all the techniques for tabular micro-data with their characteristics, advantages, and disadvantages explained in Table 1.

PRIVACY-PRESERVING TECHNIQUES FOR SOCIAL NETWORKS

Researchers had done work on privacy preserving using techniques such as k-anonymity, L-diversity, and an integrated approach of both for providing more privacy to individual while publishing data online. Social network data are defined as the network which consists of nodes and edges. A node represents individuals and edge represents some kind of connection or relationship between nodes. Fig. 2 shows a total of 5 nodes which are company A, agent 1, agent 2, agent 3, and company D and relationship between companies through agents is represented by some transactions such as 4.6, 3.9, 2.3, 9.0, 5.1, and 2.7 mm and "mm" denotes million/month. The above transactions represent the sensitive relationship between companies.

Hence, there exist various privacy preservation techniques which depend on various conditions such as to protect only individual or to protect the connection among others or both, i.e., nodes as well as relationships and connections. Depending on the information of an adversary to whom it will attack, let us start from attacking anode. Technique K-anonymity has been introduced for protecting the nodes by researchers [7,15]. The solution to protect the node came into existence against background knowledge attack. The explanation to both the techniques, i.e., K-anonymity and L-diversity is given by B.K. Treaty. Their team modified the algorithms of K-anonymity and L-diversity and he explained that the concept can be more expanded to handle a variant of multi-sensitive attributes during anonymization process [17]. The above techniques, i.e., K-anonymity and L-diversity exist for node privacy.

The anonymization methods can be broadly categorized into two sections:

1. Clustering-based approach
2. Graph modification approach.

This clustering method mainly divides nodes and edges into clusters and then anonymize a subgraph into a super-vertex. This clustering- based approach can be further categorized into various sections such as vertex clustering method, edge clustering method as well as both edge and node clustering method while another approach is the graph modification approach in which graph can be modified either by altering the vertex, edge, or by adding extra edges or vertices to the original ones [18]. Hay *et al.* [19] proposed a technique related to anonymity in which vertices look similar in nature but it will be difficult to adversary. This structural similarity called an automorphism is a vertex clustering method. He also proposed an approach of edge cluster anonymization in which aggregation of edges is done on some criteria that prevents the disclosure of sensitive connection or relationships between vertices [19]. To apply anonymization to both edge clustering and node clustering, first of all, nodes can be divided into clusters, and for anonymizing, edges in the nodes in the same cluster can be further partitioned into one single node, labeling the nodes with vertices and edges in cluster. Edges representing among two clusters are collapsed into a single edge labeling the number of edges between them [20]. Cormode studied and considered various attacks such as static as well as learned link attacks to model the knowledge of an attacker and he proposed the safe grouping mechanism applied to bipartite graph to protect privacy [21]. This is vertexes attribute mapping clustering. Punitha and Amsaveni [22] define more methods and techniques that provide more privacy in social networks. Liu and Terzi [23] proposed a method that applies dynamic programing to develop a new degree sequence which is K-degree-anonymous which also decreases the degree anonymization cost. The method comes under the optimized graph constructed approach. Panda *et al.* [24] had observed that if an adversary has some prior knowledge about the sensitive attribute, the adversary attacks it, so the concept of t-closeness has been suggested. Kavianpour *et al.* [25] proposed an algorithm that takes the benefits of both the techniques such as K-anonymity and L-diversity and it has been able to increase the level of privacy by anonymizing and diversifying the disclosed information.

Table 1: Advantages and disadvantages of privacy preservation techniques

Technique	Advantages	Disadvantages
K-anonymity	High correlation among the tuples	More number of dimensions would be violated
L-diversity	Sensitive attribute would have at most same frequency	Homogeneity and background knowledge attack have lacked
T-closeness	Measure the distance between two probabilistic distributions that were indistinguishable from one another	Information gain was unclear
K^m anonymity	Similar evaluated approach on k items	Loss of utility

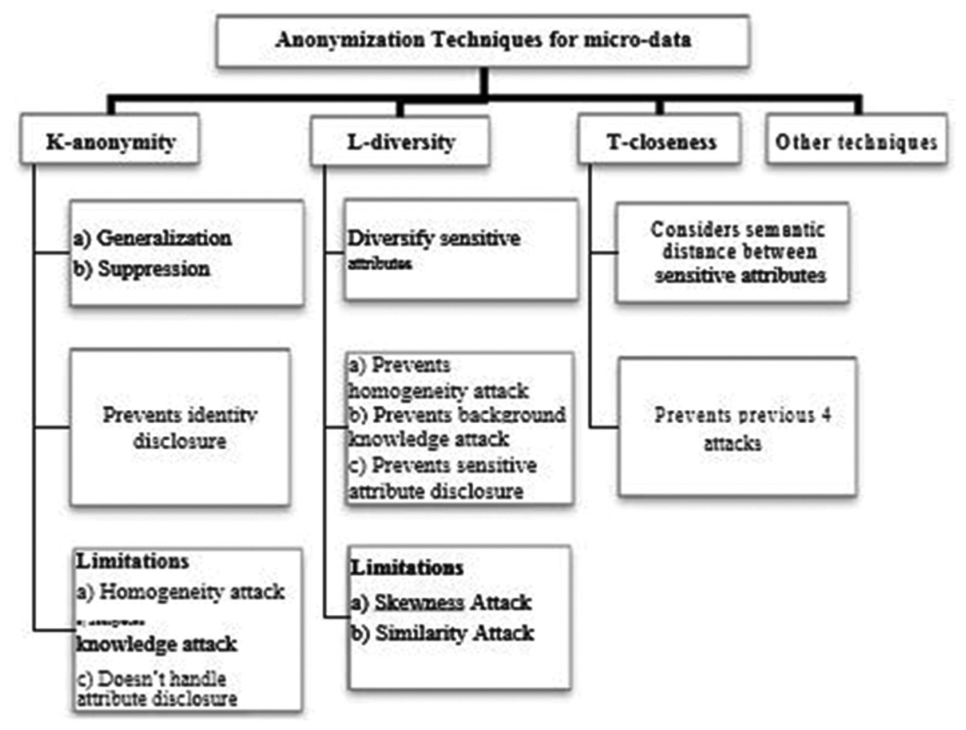
Anonymization Techniques for micro-data
K-anonymity
L-diversity
T-closeness
Other techniques
a) Generalization
b) Suppression
Prevents identity disclosure
Limitations
a) Homogeneity attack
knowledge attack
c) Doesn't handle attribute disclosure
Diversify sensitive attributes
a) Prevents homogeneity attack
b) Prevents background knowledge attack
c) Prevents sensitive attribute disclosure
Limitations
a) Skewness Attack
b) Similarity Attack
Considers semantic distance between sensitive attributes
Prevents previous 4 attacks

Fig. 1: Existing privacy preservation techniques for tabular micro-data

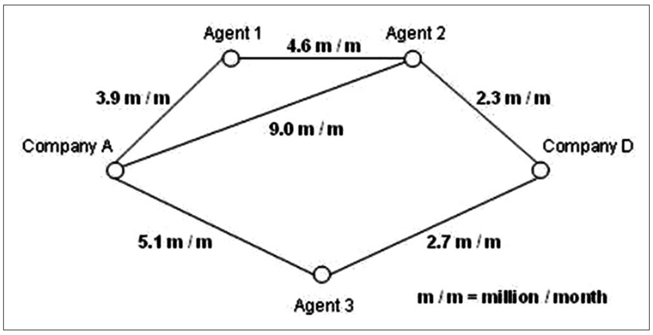

Fig. 2: Graph with sensitive information

Masoumzadeh and Joshi [26] proposed two heuristic approaches that help in preserving the structural properties of social networks by limiting the changes in shortest paths based on the metric of edge between-ness [27]. Shishodia *et al*. proposed an algorithm for achieving K-anonymity and L-diversity and it works for d>1 and they extended their work to handle a variant of multi-sensitive attributes. Their algorithm works faster than previous algorithm as significantly less number of edges is generated when applied to synthetic and real-world data sets. Other approaches come into existence are the randomized edge construction method and the randomized weight perturbation method. In randomized edge method, an anonymized graph G' is constructed by inserting "n" new edges and deleting "m" old edges. Graph can be constructed randomly and synthetically in which addition and deletion take place from the existing set of edges. Chakraborty and Annappa [28] proposed an perturbation algorithm that introduces noise in graph while preserving the local structure and other graphical properties of original graph. Their perturbation mechanism is very useful for real-world deployment of systems that leverages social links. In randomized weight perturbation approach, two existing techniques are available in which the first one is Gaussian randomization multiplication and the other one is greedy perturbation algorithm. Gaussian method mainly focuses on length of the perturbed shortest path but it does not give the guarantee of same shortest path after perturbation while greedy perturbation method not only tries to keep the length of shortest path same as that of original one but also keeps the same shortest path after perturbation as that of original one. Liu also proposed an algorithm that is based on random walk and he used matrix analysis to modify individual edge weights that keep the same shortest path as of original graph, and in this algorithm, he tries to achieve privacy through probabilistic graph [29].

There also exist more techniques that are developed but not mentioned above which are shown in Table 2.

6. RESEARCH TRENDS

Some research areas of interest in privacy preservation for social networks are as follows:

1. There exist various techniques for privacy preserving and in that utility (usefulness) of anonymized data is a serious impact. Methodologies should be developed in a way that quantitatively measure the utility of data. A method must be developed that can

Table 2: Various other privacy-preserving techniques in social networks

Year	Author	Brief description
2008	Guha *et al.* [30]	Encryption has been used to provide privacy and only authorized users can decode and decrypt the result
2008	Blosser and Zhan [31]	Proposed protocols to create and interact with privacy-preserving collaborative social networks that combines small networks together while retaining the purity of data for the owners
2008	Campan *et al.* [32]	Greedy approach to optimize utility using the attribute and structural information simultaneously has been used. Structural information loss has been introduced. SANGREEA (Social Network Greedy Anonymization)
2009	Ford *et al.* [33]	A new algorithm for enforcing p-sensitive k-anonymity on social network data based on a greedy clustering approach has been proposed
2009	Narayanan and Shmatikov [34]	Developed re-identification algorithm for anonymized graphs. Validated for Flickr and Twitter
2009	Lijie and Weining [35]	Studied link identification attack in which the adversary attacks using linking probability, t-confidence has been proposed. Dataset: EPINON, COA
2009	Fong *et al.* [36]	Proposed an access control model that generalizes the privacy preservation mechanism of Facebook
2010	Tang and Yang [37]	Introduced KNN and EBB algorithm for constructing generalized subgraphs before sharing the social network with other parties and a mechanism to integrate the generalized information to conduct the closeness centrality measures dataset: Global Salafi Jihad Terrorist SN
2010	Ding *et al.* [38]	Presented a systematic review of the existing de-anonymization attacks in online social networks
2010	Wu *et al.* [39]	Classified the existing anonymization techniques on simple graphs in three main categories: K-anonymity-based privacy preservation through edge modification, probabilistic privacy preservation through edge randomization, and privacy reservation through generalization
2011	Zheleva and Getoor [40]	Presented the literature survey on privacy in social networks, defined all the possible privacy breaches, and all the different privacy attacks have been studied
2012	Masoumzadeh ad Joshi [41]	Proposed new methods that enhance edge-perturbing anonymization on the basis of structural roles and edge between-ness in social network theory
2013	Heatherly *et al.* [42]	Observed that friendship connections and all details together give better predictability than details alone, and the effect of removing details and links in preventing sensitive information leakage has been described
2013	Cheng and Sandhu [43]	Presented a new framework that provides users control over how third party applications can access their data and activities in social networks while still retaining the functionality of third party applications
2014	Gnanasekar and Jayanthi [44]	Proposed graph anonymization technique by generalizing it, partitioning the nodes, and summarizing the graph at the partition level, and also providing protection against re-identification attacks
2014	Sun *et al.* [45]	Proposed two new heuristic algorithms that protect from mutual friend attack, and algorithms also ensure K-degree anonymity based on the K-NMF anonymity while preserving much of the utility in social networks
2015	Reddy and Shilpa [46]	Reviewed the different privacy issues related to data mining using user role-based methodology and differentiated the user roles involved in data mining applications, i.e., data provider, data collector, data miner, decision maker
2015	Kaveri and Maheswari [47]	Presented the overview of anonymization techniques and described the anonymized data in three dimensions, namely, privacy, background knowledge, and data utility
2015	Sridhar and Srinivas [48]	Developed a new data utility measurement based on graph statistics and it is used to evaluate the data utility iteratively. The procedure can be used as a benchmark process to decide when to stop further perturbation process and also can be used as a validation measure to evaluate the data utility of various existing perturbation algorithms

evaluate the various techniques in terms of tradeoff among privacy and utility.

2. Despite all the existing techniques such as k-anonymity and L-diversity, an integrated approach of K-anonymity and L-diversity has been developed for privacy preserving in social network, but the problems of privacy still exist because there is a loss of more information.
3. Different anonymization techniques have been developed so far, but all are performing operations on static datasets or single time-released dataset. However, social networking sites are generating dynamic data continuously, so new techniques should be developed to operate on dynamic datasets that provide privacy instantaneously.
4. All the privacy-preserving approaches try to evaluate the privacy in social network, taking into consideration small datasets or synthetic datasets. There is a need to perform new experiments on the existing techniques considering large datasets.
5. Many techniques exist such as K-anonymity and L-diversity that protect only nodes and only few techniques exist that provide privacy to edges such as edge perturbation and edge randomization. There is a need to develop more techniques that provide privacy by protecting sensitive edges between nodes.
6. Not even a single technique exists that prevents from all types of attacks such as homogeneity attacks, background knowledge attacks, and sensitive edge attacks. There is a need to develop a technique that gives privacy from all types of attacks.

CONCLUSION

Various techniques have been developed till now that provide privacy in tabular micro-data such as K-anonymity, L-diversity, t-closeness, and integrated approach, but all techniques have some drawbacks that lead to information loss and no technique exist that provides privacy in all aspects such as protecting nodes, protecting edges as well as both. Hence, there is a significant scope of improving the existing techniques for social data that gives minimum information loss and better utility of released data. Furthermore, there is a scope in improving the edge privacy techniques such as edge randomization and edge perturbation so that network of nodes and edges will be safe after releasing information of individual.

REFERENCES

1. Phillips E, Nurse J, Goldsmith M, Creese S. Applying social network analysis to security. Oxford, UK: ICCSS; 2015.
2. Zang L, Xu S, Bylander T, Ruan J, Krishnan R. Privacy Preserving in Social Graphs. : Citeseer; 2012.
3. Zhou B, Pei J, Luk WS. A brief survey on anonymization techniques for privacy preserving publishing of social network data. SIGKDD Explor 2008;10(2):12-22.
4. Westin AF. Privacy and Freedom. Vol. 97. London: Bodley Head; 1967.
5. Liu K, Das K, Grandison T, Kargupta H. Privacy-preserving data analysis on graphs and social networks. In: Next Generation of Data Mining. Boca Raton, FL: CRC Press; 2008. p. 419-37.
6. Fung BC, Wang K, Chen R, Yu PS. Privacy-preserving data publishing: A survey of recent developments. ACM Comput Surv (CSUR) 2010;42:1-53.
7. Samarati P, Sweeney L. Protecting privacy when disclosing information: K-anonymity and its enforcement through generalization and suppression. IEEE Trans Knowl Data Eng 2001;13(6):1010-27.
8. Machanavajjhala A, Kifer D, Gehrke J. L-diversity: Privacy beyond k-anonymity. ACM Trans Knowl Discov Data (TKDD) 2007;1(1):1-52.
9. Li N, Li T, Venkatasubramanian S. T-closeness: Privacy beyond k-anonymity and l-diversity. In: Proceedings of 23rd International Conference on Data Engineering ICDE 2007, IEEE, Istanbul; 2007. p. 106-15.
10. Sun X, Wang H, Li J, Truta TM. Enhanced P-sensitive K-anonymity models for privacy preserving data publishing. Trans Data Priv 2008;1(2):53-66.
11. Xiao X, Tao Y. M-invariance: Towards privacy preserving re-publication of dynamic datasets. In: Proceedings of International Conference on Management of Data SIGMOD ‘07. New York NY, USA: ACM; 2007. p. 689-700.
12. Chen BC, Lefevre K, Ramakrishnan R. Privacy skyline: Privacy with multidimensional adversarial knowledge. In: Proceedings of 33rd International Conference on Very Large Data Bases VLDB ‘07; 2007. p. 770-81.
13. Sweeney L. K-anonymity: A model for protecting privacy. Int J Uncertain Fuzziness Knowl Based Syst 2002;10:557-70.
14. Nergiz ME, Clifton C, Nergiz AE. Multirelational k-anonymity. IEEE Trans Knowl Data Eng 2009;21(8):1104-17.
15. Machanavajjhala A, Kifer D, Gehrke J. L-diversity: Privacy beyond k-anonymity. ACM Trans Knowl Discov Data (TKDD) 2007;1(1):1-52.
16. Li N, Li T, Venkatasubramanian S. T-closeness: Privacy beyond k-anonymity and l-diversity. In: Proceedings of 23rd International Conference on Data Engineering ICDE 2007, IEEE, Istanbul; 2007. p. 106-15.
17. Tripathy BK, Mitra A. An Algorithm to Achieve K-anonymity and l-Diversity Anonymisation in Social Networks, Fourth International Conference on Computational Aspects of Social Networks (CASoN), IEEE; 2012.
18. Zhou B, Pei J, Luk WS. A brief survey on anonymization techniques for privacy preserving publishing of social network data. SIGKDD Explor 2008;10(2):12-22.
19. Hay M, Miklau G, Jensen D, Towsley D. Resisting structural identification in anonymized social net-works. In: Proceedings of the 34th International Conference on Very Large Databases (VLDB’08). ACM; 2008.
20. Zheleva E, Getoor L. Preserving the privacy of sensitive relationships in graph data. In: Proceedings of the 1st ACM SIGKDD Workshop on Privacy, Security, and Trust in KDD (PinKDD’07); 2007.
21. Cormode G, Srivastava D, Yu T, Zhang Q. Anonymizing bipartite graph data using safe groupings. In: Proceedings of the 34th International Conference on Very Large Databases (VLDB’08). ACM; 2008.
22. Punitha N, Amsaveni R. Methods and techniques to protect the privacy information in privacy preservation data mining. Int J Comput Technol Appl 2011;2(6):2091-7.
23. Liu K, Terzi E. Towards identity anonymization on graphs. In: Proceedings of the 2008 ACM SIGMOD International Conference on Management of Data (SIG- MOD’08). New York NY, USA: ACM Press; 2008. p. 93-106.
24. Panda GK, Mitra A, Prasad A, Singh A, Gour D. Applying l-diversity in anonymizing collaborative social network. Int J Comput Sci Inf Secur 2010;8(2):324-9.
25. Kavianpour S, Ismail Z, Mohtaseb A. Preserving identity of users in social network sites by integrating anonymization and diversification algorithms. Int J Digit Inf Wirel Commun (IJDIWC) 2011;1(1):32-40.
26. Masoumzadeh A, Joshi J. Preserving structural properties in edge-perturbing anonymization techniques for social networks. IEEE Trans Dependable Secure Comput 2012;9(6):877-89.
27. Shishodia MS, Jain S, Tripathy BK. GASNA-Greedy Algorithm for Social Network Anonymization, IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining; 2013.
28. Chakraborty A, Annappa B. A perturbation based approach for privacy preserving publication of social network graphs. Karnataka: Anirban Chakraborty National Institute of Technology; 2014.
29. Liu L. Privacy Preserving Data Mining for Numerical Matrices, Social Networks and Big Data, University of Kentucy; 2015.
30. Guha S, Tang K, Francis P. NOYB: Privacy in online social networks. In: Proceedings of First Workshop on Online Social Networks WOSN’08. New York NY, USA: ACM; 2008. p. 49-54.
31. Blosser G, Zhan J. Privacy preserving collaborative social network. In: Proceedings of International Conference on Information Security and Assurance ISA 2008, Busan; 2008. p. 543-8.
32. Campan A, Truta TM, Cooper N. P-sensitive k-anonymity with generalization constraints. Trans Data Priv Arch 2008;3(2):65-89.
33. Ford R, Truta TM, Campan A. P-Sensitive k-anonymity for social networks. In: 5th International Conference on Data Mining (DMIN); 2007. p. 403-9.
34. Narayanan A, Shmatikov V. De-anonymizing social networks. In: Proceedings of 30th IEEE Symposium on Security and Privacy, Berkeley CA; 2009. p. 173-87.
35. Lijie Z, Weining Z. Edge anonymity in social network graphs. In: Proceedings of International Conference on Computational Science and Engineering CSE ‘09; 2009. p. 1-8.
36. Fong PW, Anwar M, Zhao Z. A privacy preservation model for facebook-style social network systems. In: Computer Security - ESORICS 2009, Lecture Notes in Computer Science. Vol. 5789; 2009. p. 303-320.
37. Tang X, Yang CC. Generalizing terrorist social networks with k-nearest neighbor and edge betweenness for social network integration and privacy preservation. In: Proceedings of IEEE International Conference on Intelligence and Security Informatics; 2010.
38. Ding X, Zhang L, Wan Z, Gu M. A brief survey on de-anonymization attacks in online social networks. In: Proceedings of International Conference on Computational Aspects of Social Networks, Taiyuan; 2010. p. 611-5.
39. Wu X, Ying X, Liu K, Chen L. A survey of privacy-preservation of graphs and social networks. In: Managing and Mining Graph Data, Advances in Database Systems. Vol. 40. New York: Oxford University Press; 2010. p. 421-53.
40. Zheleva E, Getoor L. Privacy in social networks: A survey. In: Social Network Data Analytics. US: Springer; 2011. p. 277-306.
41. Masoumzadeh A, Joshi J. Preserving structural properties in edge-perturbing anonymization techniques for social networks. IEEE Trans Dependable Secure Comput 2012;9(6):877-89.
42. Heatherly R, Kantarcioglu M, Thuraisingham B. Preventing private information inference attacks on social networks. IEEE Trans Knowl Data Eng 2013;25(8):1849-62.
43. Cheng Y, Sandhu R. Preserving user privacy from third-party applications in online social networks. In: Proceedings of 22nd International Conference on World Wide Web Companion, Geneva, Switzerland; 2013. p. 723-8.
44. Gnanasekar V, Jayanthi S. Privacy preservation of social network data against structural attack using k-auto restructure. Int J Comput Sci Inf Technol 2014;5(2):1375-81.
45. Sun C, Yu PS, Kong X, Fu Y. Privacy preserving social network publication against mutual friend attacks. Trans Data Priv 2014;7:71-97.
46. Reddy S, Shilpa GV. Privacy preserving publishing of social network data privacy and big data mining. Int J Emerg Technol Adv Eng 2015;5(2):126-35.
47. Kaveri VV, Maheswari V. Cluster based anonymization for privacy preserving in social network data community. J Theor Appl Inf Technol 2015;73(2):269-74.
48. Sridhar N, Srinivas Y. Preview and maximizing the data utility in privacy preserving social network. Int J Comput Appl 2015;130(3):1-5.