Privacy Preserving Techniques in Social Networks Data Publishing-A Review

Amardeep Singh
Ph.D. Scholar
Department of Computer Science
PEC University of Technology
Chandigarh, India

Divya Bansal, Ph.D
Associate Professor
Department of Computer Science
PEC University of Technology,
Chandigarh, India

Sanjeev Sofat, Ph.D
Professor
Department of Computer Science
PEC University of Technology,
Chandigarh, India

ABSTRACT

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.

General Terms

Social Network, Anonymization, Privacy, Attacks, Attributes.

Keywords

Privacy models, K-anonymity, L-diversity, t-closeness.

1. INTRODUCTION

Due to the increase in popularity of online social networks on the Web [1], large number of people subscribe to social networks or social media. This has generated large amount of user data that is gathered and maintained by the social network service providers. The data generated by social network services is termed as the social network data that needs to be published for others in certain situations. One of the situations is when specific analysis of the user data needs to be done and another situation is when the owner of the data has to share the data with third parties like advertising partners which is part of policies generally accepted by subscribers. The data contains valuable information about users that helps third parties in better social targeting of advertisements. Social network analysis is being used in modern sociology, geography, economics, and information sciences [2]. Researchers in various fields use this data for different purposes like researchers in government institutions require social network data for information and security purposes [3]. So, data needs to be shared or published in all above mentioned situations. Owner of data can publish it for others to analyze but it may create serious privacy threats. To fulfill the demands for the network data, online social media operators have been sharing the data they gather and maintain with external third parties such as advertisers, application developers, and academic researchers like Facebook has thousands of third-party applications and there has been an exponential increase in this number [4]. Social network data contains sensitive and confidential information about the users [5-7]. Thus sharing of this data in its raw form may breach privacy of individuals. Individual privacy is defined as "the right of the individual to decide what information about himself should be communicated to others and under what circumstances" [8]. A privacy breach occurs when private and confidential information about the user is disclosed to an adversary. So, preserving privacy of individuals while publishing user's collected data is an important research area. Work has been done by various researchers in this direction.

This paper is structured as follows: Section 2 describes categories of privacy breach; followed by challenges in preserving privacy in social networks data which have been briefed in Section 3; Section 4 presents exiting techniques for preserving privacy in tabular micro-data; techniques for preserving privacy in social networks has been covered in Section 5; Section 6 gives research directions for new researchers; finally Section 7 concludes the review.

2. CATEGORIES OF PRIVACY BREACH

The privacy breaches in social networks can be categorized into three types [9-10]:

i. Identity disclosure - Identity disclosure occurs when an individual behind a record is exposed. This type of breach leads to the revelation of information of a user and relationship he/she shares with other individuals in the network.

ii. Sensitive link disclosure - Sensitive link disclosure occurs when the associations between two individuals are revealed. Social activities generate this type of information when social media services are utilized by users.

iii. Sensitive attribute disclosure – Sensitive attribute disclosure takes place when an attacker obtains the information of a sensitive and confidential user attribute. Sensitive attributes may be linked with an entity and link relationship.

All these mentioned privacy breaches pose severe threats like stalking, blackmailing and robbery because users expect privacy of their data from the service provider end. Besides that it damages the image and reputation of an individual. There are many examples of accidental disclosure of private information of users' data that causes organizations to be conservative in releasing the network data, such as the AOL search data example [11] and attacks on Netflix data [12]. As per the promises of social networks there is a need to address these issues. Therefore, data needs to be released to third parties in such a way that ensures the privacy of the users. Thus data should be anonymized before releasing or publishing to third parties. But preserving privacy in social networks is difficult as mentioned in next section.

3. CHALLENGES IN PRESERVING PRIVACY IN SOCIAL NETWORK DATA PUBLISHING

Ensuring privacy for social network data is difficult than the tabular micro-data because [13]:

a) Modeling of background knowledge of adversaries is difficult in social network data than tabular micro-data. In tabular micro-data, users are identified by linking quasi-identifiers from whereas in social network information from various sources such as labels of vertices and edges, subgraphs, and neighborhood graphs can be used to identify individuals.

b) Information loss is the metric which measures the amount of distortion. In tabular micro-data information loss can be measured using the sum of information loss in individual records. Since, a social network is a graphical structure with a set of vertices and edges hence it is difficult to compare two social networks by comparing the vertices and edges individually. Anonymized social network and original social networks which have the same number of vertices and edges may have very different properties like betweenness, connectivity, and diameter. Information loss and anonymization quality can be measured in different ways.

c) Development of privacy preserving techniques in social network data is difficult than for relational data. Tabular micro-data is anonymized using divide-and-conquer techniques whereas social network is a structure of nodes and edges, any changes in labels or edges may have an effect on the neighborhoods of other vertices and edges.

The methods proposed for tabular micro-data cannot be directly applied to social network data due to the connectivity between vertices in the graph network as compared to independent nodes in tabular data. In micro-data, each tuple is independent, but the vertices and edges in a social network are linked to each other. An adversary can use the information regarding network structure to violate the privacy of users. So there is a need is to develop a technique that can ensure the privacy of the entities in social network data publishing.

4. PRVACY PRESERVING TECHNIQUES – MICRO DATA

Significant work has been done for preserving privacy in tabular micro-data. Models like K-anonymity [14][20], L-diversity [15], T-closeness [16] have been proposed which have shown good results in anonymization. Fig. 1 briefs the three models, their properties and drawbacks.

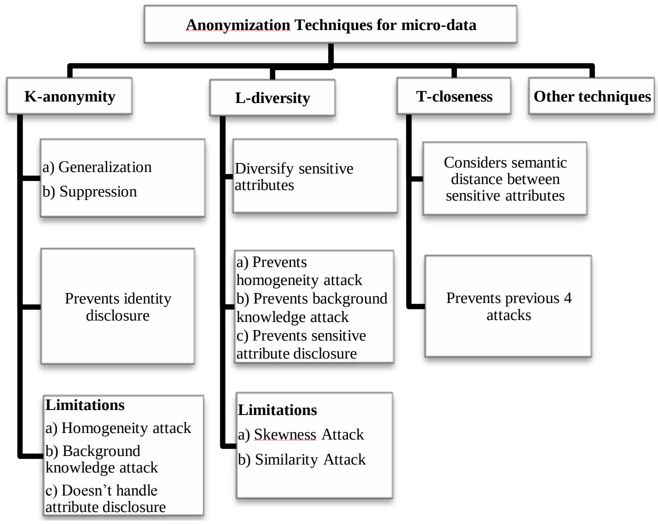
Anonymization Techniques for micro-data
K-anonymity
L-diversity
T-closeness
Other techniques
a) Generalization
b) Suppression
Prevents identity disclosure
Limitations
a) Homogeneity attack
b) Background knowledge attack
c) Doesn't handle attribute disclosure
Diversify sensitive attributes
a) Prevents 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 Preserving Techniques for Tabular micro-data

5. PRVACY PRESERVING TECHNIQUES – SOCIAL NETWORKS

Existing models of preserving privacy for micro-data have been utilized for social network data. Work has been done by various researchers using K-anonymity, L-diversity and integrated approach of K-anonymity L-diversity for protecting users' data while publishing it online. Social network data is unstructured data represented as a graph where each node/vertex represents an individual and edges represent link/association between nodes. Fig 2 shows a social network structure with 7 nodes representing individuals and salaries are sensitive attributes shown by labels. Privacy preserving techniques are based on that notion.

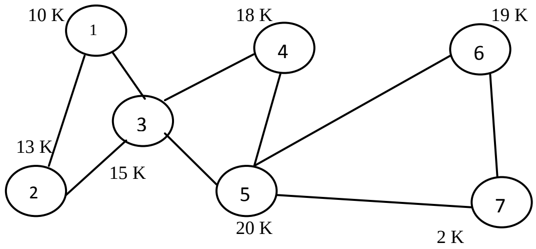

Fig. 2 Social network graph with 7 nodes and sensitive attributes as salaries

Privacy preserving techniques are developed keeping following things into consideration:

1. Adversary's knowledge
2. Utility of the data after release

So, depending upon the knowledge that an adversary uses to attack the target node following techniques have been developed by various researchers using the notion of K-anonymity [14][20]. Wei et al. [21] considered the privacy disclosure in online social network data publishing. It has been assumed that adversaries have the knowledge of the degree of a target individual and the target's immediate neighbours. A practical solution to defend against background knowledge attacks has been proposed. Anonymized social networks obtained by proposed method can be used to answer aggregate network queries with high accuracy. Social network has been modeled as an undirected labeled graph. k-subgraph has been proposed to reduce the risk of privacy disclosure in social network data publication. Zou et al. [22] proposed k-automorphism based on the assumption that the adversary has knowledge about degree, subgraph and neighbor of the target node. Tripathy et al.[23] proposed an algorithm for graph isomorphism based on adjacency matrix. It says that a subgraph is indistinguishable from at least k-1 other subgraphs. Cheng et al. [24] used K-isomorphism to preserve privacy when adversary has subgraph knowledge. Wu et al. [25] proposed k-symmetry technique to protect privacy against re-identification using subgraph information. Lan et al.[26] developed an algorithm called KNAP against 1-neighborhood attack for publishing social networks data. Skarkala et al. [27] applied K-anonymity to weighted social networks. Liu et al. [28] proposed the concept of k-degree to prevent vertex re-identification through the information of vertex degree.

Preserving privacy in social networks using k-anonymity protects against linking disclosure but still it may leak privacy under the cases of homogeneity and background knowledge attacks. Moreover, K-anonymity doesn't protect against attribute disclosure. So, L-diversity was developed by Machanavajjhala [15] in year 2007.

Panda et al. [29] used a new practical and efficient definition of privacy called l-diversity on preserving privacy in collaborative social network data and the effect on the utility of the data for social network analysis has been seen. It has been identified that l-diversity social network still may leak privacy as an adversary may have some prior knowledge about the sensitive attribute value of an individual before seeing the released table. After seeing the released table, the adversary may have a posterior knowledge. Information gain i,e., the difference between the posterior knowledge and the prior knowledge is the factor to leak privacy. So the concept of t-closeness has been suggested to be introduced. Li et al. [30] proposed to preserve relationship privacy between two users one of whom can be identified in the released social network data. l-diversity anonymization model has been defined to preserve users' relationship privacy. Two graph manipulation algorithms, MaxSub and MinSuper, have been proposed to achieve l-diversity anonymization.

Then, to preserve privacy in better way integrated approach of K-anonymity and L-diversity has been suggested by few authors as mentioned below.

Kavianpour et al. [31] proposed an integrated algorithm that takes the advantages of K-anonymity and l-diversity algorithm then evaluated the effectiveness of the combined strengths. Proposed algorithm has been able to increase the level of privacy for social network users by anonymizing and diversifying disclosed information. Tripathy et al. [32] proposed an algorithm which follows k-anonymity and l-diversity properties and can handle a variant of multisensitive attributes during anonymization process. Proposed algorithm is modified form of corresponding algorithms for micro data and it also depends upon some modified algorithms developed for anonymization against neighbourhood attacks. Drawback of proposed algorithm is that it still needs some improvements in order to reduce the complexity so that it can be applied to large social networks. Yuan et al. [33] defined a k-degree l-diversity anonymity model for the protection of structural information and sensitive labels of people. Many privacy models like k-anonymity to prevent node reidentification through structure information have been proposed but an attacker may still be able to obtain private information of a person i.e. the label-node relationship is not well protected by pure structure anonymization methods. An anonymization methodology has been proposed by adding noise nodes into the original graph with the consideration of introducing the least distortion to graph properties.

Other than above mentioned techniques for preserving privacy other techniques have also been proposed and developed as shown in table 1.

Table 1. Various Other Privacy Preserving Techniques in Social Networks

Year	Author	Brief
2008	Zhou et al. [34]	Reviewed existing anonymization techniques for privacy preserving publishing of social network data.
2008	Guha et al. [35]	Encryption has been used to provide privacy and only authorized users can decode and decrypt the result.
2008	Blosser et al. [36]	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. [37]	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).
2008	Zheleva et al. [38]	How to preserve sensitive relationships.
2009	Ford et al. [39]	A new algorithm for enforcing p-sensitive k-anonymity on social network data based on a greedy clustering approach has been proposed .
2009	Narayanan et al. [40]	Developed Re-identification algo for anonymized graphs. Validated for Flickr and Twitter.
2009	Lijie et al. [41]	Studied link identification attack in which the adversary attacks using linking probability, *t*-confidence has been proposed. Dataset: EPINON, COA
2009	Ying et al. [42]	Considered edge re-identification attacks when the adversary has no background knowledge Dataset: Enron, Email,Polblogs, Polbooks.
2009	Tootoonchian et al.[43]	Presented Lockr, a system that improves the privacy of centralized online system like Flickr and decentralized online content sharing systems like BitTorrent.
2009	Fong et al. [44]	Proposed an access control model that generalizes the privacy preservation mechanism of Facebook.
2010	Tang et al. [45]	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 Salfi Jihad Terrorist SN.
2010	Lan et al. [46]	Proposed an approach for preserving privacy of social networks which can be represented as bipartite graphs. Synthetic dataset
2010	Ding et al. [47]	Presented a systematic review of the existing de-anonymization attacks in online social networks.
2010	Sun et al. [48]	Proposed a privacy-preserving method for sharing data in social networks, with efficient revocation for preventing a contact's access right to the private data once the contact is removed from the social group and can be used as a plug-in for Facebook.
2010	Beach et al. [49]	q-Anon model has been presented to measure the probability of an attacker to identify unknown information from a social network API with the assumption that the data being protected may already be public. Validated on Facebook for 700 users
2010	Zhu et al. [50]	Proposed a collaborative framework for access control in social networks through an innovative key management.
2010	Wu et al. [51]	**C**ategorized the existing anonymization methods on simple graphs in 3 main categories: K-anonymity based privacy preservation via edge modification, probabilistic privacy preservation via edge randomization, privacy reservation via generalization.
2011	Yang et al. [52]	Non sensitive and generalized information has been used to support social network analysis and mining and to preserves the privacy of information.
2011	Zheleva et al. [53]	Surveyed the literature on privacy in social networks, Possible privacy breaches have been defined and possible privacy attacks have been studied.
2012	Fire et al. [54]	Developed Social Privacy Protector, software which aims to improve the security&privacy of Facebook users.
2012	Masouzadeh et al. [55]	Proposed methods to enhance edge-perturbing anonymization on the basis of structural roles and edge betweenness in social network theory. Dataset: Polbook, Jazz
2013	Tassa et al. [56]	The first study of privacy preservation in distributed social networks which s shown to outperform SaNGreeA algorithm which is the leading algorithm for achieving anonymity in networks by means of clustering
2013	Heathely et al. [57]	Examined that friendship links and details altogether provide better predictability than details alone, effect of removing details and links in preventing sensitive information leakage has been explored.
2013	Cheng et al. [58]	Proposed a framework to provide users controls over how third party applications can access their data and activities in social networks while still retaining the functionality of third party applications.

6. RESEARCH DIRECTIONS

Following are the few inferences drawn from literature survey:

1. To preserve usefulness(utility) of anonymized data is an important aspect while applying techniques for privacy preservation. So, there is a need to develop methodologies that can quantitatively measure utility of data. There is need to evaluate various techniques in terms of tradeoff between privacy and utility.
2. Many algorithms like k-anonymity, L-diversity, integrated approach of k-anonymity & L-diversity have been developed for preserving privacy of social network user data but existing techniques leads to substantial information loss.
3. Anonymization techniques have been developed for one time released network data. But many applications require publishing data periodically so there is a need to develop techniques that can preserve privacy of dynamic releases.
4. Techniques are available for preserving privacy in case of distributed tabular data e.g. [59]. However, in case of social network distributed privacy preserving techniques are not well reported in literature except [56].
5. Existing privacy preserving approaches for social networks have been evaluated using either small datasets or synthetic datasets. There is need to conduct empirical experiments on large datasets.
6. There is no existing technique which can prevent homogeneity attacks, background knowledge attacks, attacks arising due to distance between sensitive values.

7. CONCLUSION

It became evident from the literature that privacy of users is the main concern and topic of research now a days. Various models proposed for tabular micro-data have been adopted for preserving privacy of social network data. Techniques like K-anonymity, L-diversity, integrated K-anonymity L-diversity have been used till now but these techniques lead to substantial information loss. So, there is a scope of improvement of the techniques that provide privacy preservation with minimum information loss and better utility of released data.

8. REFERENCES

[1] Alexa 2013, The top 500 sites on the web, Available: http://www.alexa.com/topsites

[2] B. Zhou, Jian Pei, Wo-Shun Luk, "A brief survey on anonymization techniques for privacy preserving publishing of social network data," ACM SIGKDD Explorations Newsletter, Vol. 10, pp. 12-22, 2008.

[3] D. Rosenblum, "What anyone can know: The privacy risks of social networking sites," In: IEEE Security & Privacy, Vol. 5, Issue 3, pp 40-49, 2007.

[4] A. Narayanan, V. Shmatikov, "De-anonymizing social networks", In Proc of 30th IEEE Symposium on Security and Privacy, Berkeley, CA, pp 173-187, 2009.

[5] J. M. Kleinberg, "Challenges in mining social network data: processes, privacy, and paradoxes," In Proc. of 13th ACM SIGKDD International conference on Knowledge discovery and data mining, ACM New York, NY, USA, pp 4-5, 2007.

[6] L. Backstrom, Cynthia Dwork, Jon Kleinberg, "Wherefore art thou r3579x?: anonymized social networks, hidden patterns, and structural steganography," In Proc. of 16th International conference on World Wide Web, ACM, New York, NY, USA , pp 181-190, 2007.

[7] Jaideep Srivastava, Muhammad A. Ahmad, Nishith Pathak, David Kuo-Wei Hsu, "Data mining based social network analysis from online behavior," SIAM conference on Data Mining, 2008.

[8] A. F. Westin, Privacy and freedom vol. 97: London, 1967.

[9] Kun Liu, Kamalika Das, Tyrone Grandison, Hillol Kargupta, "Privacy-preserving data analysis on graphs and social networks," In: Next Generation of Data Mining, pp. 419-437, 2008.

[10] E. Zheleva, L. Getoor, "Preserving the privacy of sensitive relationships in graph data," In: Privacy, Security, and Trust in KDD, Lecture Notes in Computer Science, Vol. 4890, pp 153-171, 2008.

[11] S. Hansell, "AOL removes search data on vast group of web users," New York Times, 2006.

[12] Facebook (2013, Facebook Statistic. Available: http://www.facebook.com/press/info.php/statistics

[13] Benjamin C. M. Fung, Ke Wang, Rui Chen, Philip S. Yu, "Privacy-preserving data publishing: A survey of recent developments," In: ACM Computing Surveys (CSUR), Vol. 42, pp 1-53, 2010.

[14] P. Samarati, L. Sweeney, "Protecting privacy when disclosing information: k-anonymity and its enforcement through generalization and suppression," In: IEEE Transactions on Knowledge and Data Engineering, 2001.

[15] Ashwin Machanavajjhala, Daniel Kifer, Johannes Gehrke, "l-diversity: Privacy beyond k-anonymity," In: ACM Transactions on Knowledge Discovery from Data (TKDD), vol. 1, 2007.

[16] Ninghui Li, Tiancheng Li, Suresh Venkatasubramanian, "t-closeness: Privacy beyond k-anonymity and l-diversity," In Proc. of 23rd International Conference on Data Engineering ICDE 2007, IEEE, Istanbul, pp 106-115, 2007.

[17] Xiaoxun Sun, Hua Wang, Jiuyong Li, Traian Marius Truta, "Enhanced P-sensitive K-anonymity models for privacy preserving data publishing," In: Transactions on Data Privacy, vol. 1, pp 53-66, 2008.

[18] X. Xiao, Y. Tao, "M-invariance: towards privacy preserving re-publication of dynamic datasets," In Proc. of International conference on Management of data SIGMOD '07, ACM, New York, NY, USA, pp 689-700, 2007.

[19] Bee-Chung Chen, Kristen LeFevre, Raghu Ramakrishnan, "Privacy skyline: Privacy with multidimensional adversarial knowledge," In Proc. of 33rd International conference on Very large data bases VLDB '07, pp 770-781, 2007.

[20] L. Sweeney, "k-anonymity: A model for protecting privacy," In: International Journal of Uncertainty Fuzziness and Knowledge Based Systems, Vol. 10, pp. 557-570, 2002.

[21] Qiong Wei, Yansheng Lu, "Preservation of Privacy in Publishing Social Network Data", In Proc. of International Symposium on Electronic Commerce and Security, Guangzhou City, pp 421 - 425, 2008.

[22] L. Zou, L. Chen, M. T. Ä Ozsu, "K-automorphism: A general framework for privacy preserving network publication", In Proc. of 35th International Conference on Very Large Data Base, Vol. 2, pp 946-957, 2009.

[23] B. K. Tripathy, G. K. Panda, "A New Approach to Manage Security against Neighborhood Attacks in Social Networks", In Proc. of International Conference on Advances in Social Networks Analysis and Mining (ASONAM), Odense, pp 264 – 269, 2010.

[24] J.Cheng, AdaWai-cheeFu, Jia Liu, "K-isomorphism: privacy preserving network publication against structural attacks," In Proc. of the 2010 ACM SIGMOD International Conference on Management of data, pp. 459-470, 2010.

[25] W. Wu, Yanghua Xiao, Wei Wang, Zhenying He, Zhihui Wang "k-symmetry model for identity anonymization in social networks," In Proc. of the 13th International Cojucbybgnference on Extending Database Technology, ACM, New York, USA, pp 111-122, 2010.

[26] Lihui Lan, Hua Jin, Yang Lu, "Personalized anonymity in social networks data publication", In Proc. of IEEE International Conference on Computer Science and Automation Engineering (CSAE), Shanghai, pp 479 - 482, 2011.

[27] Maria Eleni Skarkala, Manolis Maragoudakis, Stefanos Gritzalis, Lilian Mitrou, Hannu Toivonen, Pirjo Moen, " Privacy Preservation by K-Anonymization of weighted Social Networks", ASONAM, pp 423-428. In IEEE Computer Society, 2012.

[28] K. Liu, E. Terzi, "Towards identity anonymization on graphs," In Proc. of 2008 ACM SIGMOD International conference on Management of data, Vancouver, Canada, 2008

[29] G.K.Panda, A. Mitra, Ajay Prasad, Arjun Singh, Deepak Gour, "Applying l-Diversity in anonymizing collaborative social network" In: International Journal of Computer Science and Information Security, Vol 8, Issue 2, pp 324 - 329, 2010.

[30] Na Li, Nan Zhang, Sajal K. Das, "Relationship Privacy Preservation in Publishing Online Social Networks", In Proc. of IEEE International Conference on Privacy, Security, Risk, and Trust, Boston, MA, pp 443-450, 2011.

[31] Sanaz Kavianpour, Zuraini Ismail, and Amirhossein Mohtaseb, "Preserving Identity Of Users In Social Network Sites By Integrating Anonymization And Diversification Algorithms", In: International Journal of Digital Information and Wireless Communications (IJDIWC), Hongkong, Vol. 1, Issue 1, pp 32-40, 2011.

[32] B. K. Tripathy, Anirban Mitra, "An Algorithm to achieve k-anonymity and l-diversity anonymisation in Social Networks", In Proc. of Fourth International Conference

on Computational Aspects of Social Networks (CASoN), Sao Carlos, pp 126 – 131, 2012.

[33] Mingxuan Yuan, Lei Chen, Philip S. Yu, Ting Yu, “Protecting Sensitive Labels in Social Network Data Anonymization”, In: IEEE Transactions On Knowledge And Data Engineering, Vol. 25, No. 3, pp 633-647, 2013.

[34] B. Zhou, Jian Pei, Wo-Shun Luk, "A brief survey on anonymization techniques for privacy preserving publishing of social network data," ACM SIGKDD Explorations Newsletter, Vol. 10, pp. 12-22, 2008.

[35] Saikat Guha, Kevin Tang, Paul Francis, “NOYB: Privacy in Online Social Networks”, in Proc. of first workshop on Online social networks WOSN’08, ACM New York, NY, USA, pp 49-54, 2008.

[36] Gary Blosser, Justin Zhan, “Privacy Preserving Collaborative Social Network”, In Proc. of International Conference on Information Security and Assurance ISA 2008, Busan, pp, 543 - 548, 2008.

[37] Alina Campan, Traian Marius Truta, Nicholas Cooper, “P-Sensitive K-Anonymity with Generalization Constraints”, In: Transactions on Data Privacy archive, Vol. 3 Issue 2, pp 65-89, 2010.

[38] Elena Zheleva, Lise Getoor, “Privacy in Social Networks: A Survey”, In: Social Network Data Analytics, Springer US, pp 277-306, 2011.

[39] Roy Ford, Traian Marius Truta, and Alina Campan, “P-Sensitive K-Anonymity for Social Networks”.

[40] A. Narayanan, V. Shmatikov, "De-anonymizing social networks”, In Proc of 30th IEEE Symposium on Security and Privacy, Berkeley, CA, pp 173-187, 2009.

[41] Z. Lijie and Z. Weining, "Edge Anonymity in Social Network Graphs," in Proc. of International Conference on Computational Science and Engineering CSE '09, pp 1-8, 2009.

[42] X. Ying and X. Wu, "On link privacy in randomizing social networks," In: Advances in Knowledge Discovery and Data Mining, pp. 28-39, 2009.

[43] Amin Tootoonchian, Stefan Saroiu, Yashar Ganjali, Alec Wolman, “Lockr: Better Privacy for Social Networks”, in Proc. of the 5th ACM International Conference on Emerging Networking Experiments and Technologies (CoNEXT), 2009.

[44] Philip W. L. Fong, Mohd Anwar, and Zhen Zhao, “A Privacy Preservation Model for Facebook-Style Social Network Systems”, In: Computer Security - ESORICS 2009, Lecture Notes in Computer Science, Vol. 5789, 2009, pp 303-320, 2009.

[45] X. Tang and C.C. Yang, "Generalizing Terrorist Social Networks with K-Nearest Neighbor and Edge Betweenness for Social Network Integration and Privacy Preservation," In Proc. of IEEE International Conference on Intelligence and Security Informatics, 2010.

[46] Lihui Lan, Shiguang Ju Hua Jin, “Anonymizing Social Network using Bipartite Graph”, In Proc. of International Conference on Computational and Information Sciences (ICCIS), Chengdu, pp 993 - 996, 2010.

[47] Xuan Ding, Lan Zhang, Zhiguo Wan, and Ming Gu, “A Brief Survey on De-anonymization Attacks in Online Social Networks”, In Proc. of International Conference on Computational Aspects of Social Networks, Taiyuan, pp 611 - 615, 2010.

[48] Jinyuan Sun, Xiaoyan Zhu, and Yuguang Fang, “A Privacy-Preserving Scheme for Online Social Networks with Efficient Revocation”, In Proc. of INFOCOM, IEEE, San Diego, CA, pp 1-9, 2010.

[49] Aaron Beach, Mike Gartrell, Richard Han, “q-Anon: Rethinking Anonymity for Social Networks”, In Proc. of IEEE Second International Conference on Social Computing (SocialCom), Minneapolis, MN, pp 185 – 192, 2010.

[50] Yan Zhu, Zexing Hu, Huaixi Wang, Hongxin Hu, Gail-Joon Ahn, “A Collaborative Framework: for Privacy Protection in Online Social Networks”, In Proc. of 6th International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom), Chicago, IL, pp 1 – 10, 2010.

[51] Xintao Wu, Xiaowei Ying, Kun Liu, ,Lei Chen, “A Survey of Privacy-Preservation of Graphs and Social Networks”, In : Managing and Mining Graph Data, Advances in Database Systems, Vol. 40, pp 421-453, 2010.

[52] Christopher C. Yang , “Preserving privacy in social network integration with τ-tolerance”, In Proc. of IEEE International Conference on Intelligence and Security Informatics (ISI), Beijing, pp 198 – 200, 2011 .

[53] Elena Zheleva, Lise Getoor, “Privacy in Social Networks: A Survey”, In: Social Network Data Analytics, Springer US, pp 277-306, 2011.

[54] Michael Fire, Dima Kagan, Aviad Elishar, and Yuval Elovici, "Social Privacy Protector - Protecting Users’ Privacy in Social Networks,",In Proc. of the Second International Conference on Social Eco-Informatics (SOTICS), Venice, Italy, 2012.

[55] Amirreza Masoumzadeh, James Joshi, “Preserving Structural Properties in Edge-Perturbing Anonymization Techniques for Social Networks”, In: IEEE Transactions On Dependable And Secure Computing, Vol. 9, No. 6, pp 877-889, 2012.

[56] Tamir Tassa, Dror J. Cohen, “Anonymization of Centralized and Distributed Social Networks by Sequential Clustering”, In: IEEE Transactions On Knowledge And Data Engineering, Vol. 25, No. 2, pp 311- 324, 2013.

[57] Raymond Heatherly, Murat Kantarcioglu, and Bhavani Thuraisingham, “Preventing Private Information Inference Attacks on Social Networks”, In: IEEE Transactions On Knowledge And Data Engineering, Vol. 25, No. 8, pp 1849-1862, 2013.

[58] Yuan Cheng, Ravi Sandhu, “Preserving User Privacy from Third-party Applications in Online Social Networks, In Proc. of 22nd international conference on World Wide Web companion, Geneva, Switzerland, pp 723-728, 2013.

[59] Y. Lindell and B. Pinkas, “Privacy preserving data mining” In: Advances in Cryptology CRYPTO'00, Springer-Verlag, pp 36-53, 2000.