ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 1, Issue 8, October 2013

Certain Investigations on Approaches for Protecting Graph Privacy in Data Anonymization

S.Charanyaa[1] T.Shanmugapriya[2]

M.Tech. Student, Dept. of Information Technology, S.N.S. College of Technology, Coimbatore, TamilNadu, India[1]

Assistant Professor, Dept. of Information Technology, S.N.S. College of Technology, Coimbatore, TamilNadu, India[2]

ABSTRACT: Developing privacy preserving mechanisms for data sharing across network for research purposes and business decisions has become one of the issues of the days research interest. L.Sweeney et.al., (2002) [26] developed the concept of k-anonymity, a model for protecting privacy which poses the condition that a database to be k-anonymous, then each record is indistinguishable from at least k-1 other records with respect to their quasi-identifiers. Despite the k-anonymity model, an intruder may gain access the sensitive information if a set of nodes share similar attributes. In this paper we systematically analyze the pure structure anonymization mechanisms and models proposed in the literature. Also we make a detailed study on k-degree-l-diversity anonymity model, which takes into consideration the structural information and sensitive labels of individuals as well. Also the study the algorithmic impact of adding noise nodes to original graph and the rigorous analyses on the theoretical limitations of the appended noise nodes and its impact.

K*eywords*: Sensitive information, k-anonymity, l-diversity, Database Privacy, Security

I. INTRODUCTION

Usage of Facebook, LinkedIn and more networking sites have increased extravagantly in the recent years. Due to this steep rise, there is a great opportunity for the intruders to gain useful information such as behavioral pattern of user, growth of a community, spreading of a particular disease in a geographical area. Such private information of the individuals must be preserved in social networking sites the key challenge appears in ensuring privacy and utility as well. We make a detailed investigations on a spectrum of privacy models and graphical model where the node of a graph indicates a sensitive attribute. Recently a lot of works have been done on anonymizing a relational database. k-anonymity approach developed by L.Sweeney et.al., (2001) [26] , a model for protecting privacy which poses the condition that a database to be k-anonymous, then each record is indistinguishable from at least k-1 other records with respect to their quasi-identifiers. Quasi-Identifiers are attributes whose values when taken together can potentially identify an individual. Since k-anonymity failed to secure the attribute disclosure, and is susceptible to homogeneity attack and background knowledge attack A.Machanavajjhala et.al.,[20] (2006) introduced a new privacy notation called 'l-diversity'. An equivalence class is said to possess l-diversity if there are atleast 'l' well represented values for the sensitive attribute. A table is said to have l-diversity if every equivalence class of the table has l-diversity. Privacy is measured by the information gain of an observer. Before seeing the released table the observer may think that something might happen to the sensitive attribute value of a single person. After seeing the released table the observer may have the details about the sensitive attributes. t-closeness should have the distance between the class and the whole table is no more than a threshold t, Ningui Li et.al.,[17] (2010). Graph structures are also published hand-in-hand when publishing social network data as it may be exploited to compromise privacy. The degree and subgraph of a node could be used to identify a node. It is observed from literature that inorder to prevent structure attacks the graph is enforced to satisfy k-anonymity.

The remainder of the paper is organized as follows. Basic definition and primitives of privacy preserving databases are dealt in detail in Section 2. Section 3 gives the survey on applications where node with sensitive

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 1, Issue 8, October 2013

attributes should be published. Section 4 briefs about clustering and edge editing approaches for protecting graph privacy. Section 5 concludes the paper and outlines the future work.

II. BASIC DEFINITION AND PRIMITIVES

Data refers to organized personal information in the form of rows and columns. Row refers to individual tuple or record and column refers to the field. Tuple that forms a part of a single table are not necessarily unique. Column of a table is referred to as attribute that refers to the field of information, thereby an attribute can be concluded as domain. It is necessary that attribute that forms a part of the table should be unique. According to L.Sweeney et.al., (2001) [26] each row in a table is an ordered n-tuple of values $<d_1,d_2,....d_n>$ such that each value d_j forms a part of the domain of j^{th} column for j=1,2,...n where 'n' denoted the number of columns.

A. ATTRIBUTES

Consider a relation $R(a_1, a_2,... a_n)$ with finite set of tuples. Then the finite set of attributes of R are $\{a_1, a_2,... a_n\}$, provided a table $R(a_1, a_2,... a_n)$, $\{a_1, a_2,... a_i\} \subseteq \{a_1, a_2,... a_n\}$ and a tuple $l \in R$, $l[a_i,... a_n]$ corresponds to ordered set of values $v_i,...v_j$ of $a_i... a_j$ in l. R $[a_i... a_j]$ corresponds to projection of attribute values $a_1, a_2,...,a_n$ in R, thereby maintaining tuple duplicates.

According to Ningui Li, Tiancheng Li et.al., [17] (2010), attributes among itself can be divided into 3 categories namely
1. Explicit identifiers- Attributes that clearly identifies individuals. For eg, Social Security Number for a US citizen.
2. Quasi identifiers- Attributes whose values when taken together can potentially identify an individual. Eg., postal code, age, sex of a person. Combination of these can lead to disclosure of personal information.
3. Sensitive identifiers- That are attributes needed to be supplied for researchers keeping the identifiers anonymous. For eg, 'disease' attribute in a hospital database, 'salary' attribute in an employee database.

Table 1:
Microdata Database containing sensitive Information

Race	Birth	Gender	Zipcode	Disease (Sensitive Information)
Black	1965	M	0213	Shortbreath
Black	1965	M	0213	Shortbreath
Black	1965	M	0214	Hypertension
White	1964	F	0213	Obesity
White	1965	F	0214	Chestpain
White	1967	M	0213	Shortbreath
White	1964	M	0214	Chestpain

B. QUASI- IDENTIFIERS

As proposed by L.Sweeney et.al., (2001) [26], A single attribute or a set of attributes that, in combination with some outside world information that can identify a single individual tuple in a relation is termed as quasi-identifier. Given a set of entities E, and a table $B(a_1,\ldots,a_n)$, f_a: E→B and f_b: B → E', where E → E'. A quasi-identifier of B, written as U_E, is a set of attributes $\{a_i,\ldots,a_j\} \rightarrow \{a_1,\ldots,a_n\}$ where: $\exists s_i \in U$ such that $f_a(f_b(s_i)[U_E]) = s_i$.

C. K-ANONYMITY

Let RT(A1,A2,….An) be a table and QI_{RT} be the Quasi identifier. RT is said to be k-anonymous [26] if and only if each sequence of values in $RT[QI_{RT}]$ appears atleast k-times in $RT[QI_{RT}]$. In short, the Quasi identifier must appear atleast 'k' times in RT, where k=1,2,3,... where 'k' is termed to be the anonymity of the table.

D. L-DIVERSITY

Since k-anonymity failed to secure the attribute disclosure, and is susceptible to homogeneity attack and background knowledge attack A.Machanavajjhala et.al, (2006) [38] introduced a new privacy notation called 'l-diversity'[20]. An

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 1, Issue 8, October 2013

equivalence class is said to possess l-diversity if there are atleast 'l' well represented values for the sensitive attribute. A table is said to have l-diversity if every equivalence class of the table has l-diversity. Here the technique is the sensitive attribute in each equivalence class is distributed with l-well represented values. Generally there are four types of l-diversity.

1) Distinct l-diversity: This ensures that there are atleast l-distinct values for the sensitive attribute in each equivalence class. The biggest disadvantage here is that distinct l-diversity fails to prevent probabilistic inference attacks.

2) Probabilistic l-diversity: An anonymised table is said to be probabilistic l-diversity if the frequency of the sensitive value in each group is atmost 1/l.

3) Entropy l-diversity: It is defined by, Entropy (E)$= -\sum_{s\in S} P(E,s)\log p(E,s)$, where 's' is the sensitive attribute.

4) Recursive(c,l) diversity: This technique proceeds by making, the value appearing most frequently, not appear too frequently and less frequently appearing value not to appear too rarely.

One problem with l-diversity is that it is limited in its assumption of adversarial knowledge. l-diversity fails to prevent attribute disclosure and is susceptible to two types of attacks.

E. t-Closeness

Privacy is measured by the information gain of an observer. Before seeing the released table the observer may think that something might happen to the sensitive attribute value of a single person. After seeing the released table the observer may have the details about the sensitive attributes. t-closeness [17] should have the distance between the class and the whole table is no more than a threshold t, Ningui Li et.al., (2010)[17].

In the following section we will describe various stages involved in the drowsiness detection system.

III. NEED FOR SENSITIVE ATTRIBUTES IN APPLICATIONS

A. Campan, T.M. Truta, and N. Cooper (2010) [5] have proposed a new approach for privacy preserving, where requirements on the quantity of deformation allowed on the initial data are forced in order to preserve its usefulness. Their approach consists of specifying quasiidentifiers' generalization constraints, and achieving p-sensitive k-anonymity within the imposed constraints. According to their point of view, limiting the amount of allowed generalization when masking microdata is essential for real life datasets. They formulated an algorithm for generating constrained p-sensitive k-anonymous microdata and named it as constrained p-sensitive k-anonymity model, and proved that the algorithm is in par with other similar algorithms existing in the literature in terms of quality of result.

B. Zhou and J. Pei (2011) [33] took initiative toward preserving privacy in social network data. In specific the authors identified and focused on an essential type of privacy attacks called neighborhood attacks. If an adversary has certain knowledge about the neighbors of a target victim and the relationship among the neighbors, the victim may be re-identified from a social network even if the victim's identity is preserved using the conventional anonymization techniques.

Inorder to protect privacy against neighborhood attacks, the authors extended the conventional k-anonymity and l-diversity models from relational data to social network data and also proved that the problems of computing optimal k-anonymous and l-diverse social networks are NP-hard. Authors formulated realtime solutions to problems that inferred that the anonymized social network data by proposed method can be employed to answer aggregate network queries with high degree of accuracy.

K. Liu and E. Terzi (2008) [18] and M. Hay, G. Miklau, D. Jensen, D. Towsley, and P. Weis (2008) [15] enunciated degree-attack, one of the popular attacks methods , to prove that mechanisms could be designed to protect both identities and sensitive labels. Other types of attacks such as subgraph query attacks or hub node query attacks is studied by M. Hay, G. Miklau, D. Jensen, D. Towsley, and P. Weis (2008) [15]

IV. APPROACHES FOR PROTECTING GRAPH PRIVACY

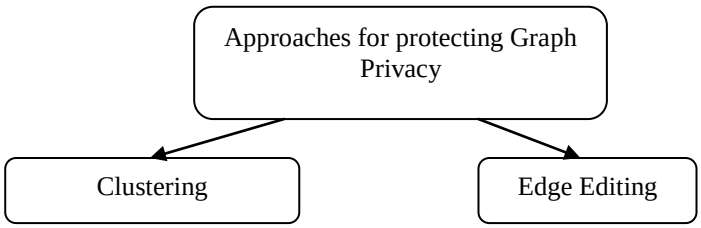
Current approaches for protecting graph privacy can be classified into two categories: clustering and edge editing.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 1, Issue 8, October 2013



A. CLUSTERING APPROACH FOR PROTECTING GRAPH PRIVACY

Clustering method is carried out by merging a subgraph to one super node, which is unsuitable for sensitive labeled graphs, because when a group of nodes are merged into a single super node, the node-label relations have been lost.

G. Cormode, D. Srivastava, T. Yu, and Q. Zhang (2008) [7] introduced a new family of anonymizations, for bipartite graph data, called (k,l)-groupings. These groupings preserve the fundamental graph structure completely, and instead anonymize the mapping from entities to nodes of the graph. Authors identified a class of "safe" (k,l)-groupings that have provable guarantees to resist a variety of attacks, and show how to find such safe groupings. Their experiments on real bipartite graph data to study the utility of the anonymized version, and the impact of publishing alternate groupings of the same graph data demonstrated that (k,l)-groupings offer significantly good tradeoffs between privacy and utility E. Zheleva and L. Getoor (2007)[30] threw light on the problem of preserving the privacy of sensitive relationships in graph data.In specific the authors dealt with the problem of inferring sensitive relationships from anonymized graph data as link reidentification. We propose five different privacy preservation strategies, which vary in terms of the amount of data removed, data utility and the amount of privacy preserved as well. Their experimental investigation revealed the victory of several re-identification strategies under varying structural characteristics of the data.

A. Campan and T.M. Truta (2008) [4] contributed in the development of a greedy privacy algorithm for anonymizing a social network and the introduction of a structural information loss measure that quantifies the amount of information lost due to edge generalization in the anonymization process. The authors proposed SaNGreeA (Social Network Greedy Anonymization) algorithm, which performs a greedy clustering processing to generate a k-anonymous masked social network and quantified the generalization information loss and structural information loss. Clustering-based model is to cluster "similar" nodes together to form super nodes. Each super node represents several nodes which are also called a "cluster." Then, the links between nodes are represented as the edges between super nodes which is called "super edges." Each super edge may represent more than one edge in the original graph. A clustered graph is a graph which contains only super nodes and super edges (2013) [35].

B. EDGE EDITING APPROACH FOR PROTECTING GRAPH PRIVACY

Edge-editing methods keep the nodes in the original graph unchanged and only add/delete/swap edges. K.B. Frikken and P. Golle (2006) [10] proposed a method to reconstructing the whole graph privately, i.e., in a way that hides the correspondence between the nodes and edges in the graph and the real-life entities and relationships that they represent to assuage these privacy concerns. Authors first represent the privacy threats posed by the private reconstruction of a distributed graph. Proposed model takes into account the possibility that malicious nodes may report incorrect information about the graph in order to facilitate later attempts to de-anonymize the reconstructed graph. Also the authors propose protocols to privately assemble the pieces of a graph in ways that diminish these threats. These protocols substantially restrict the ability of adversaries to compromise the privacy of truthful entities.

X. Ying and X. Wu (2008) [29] successfully investigated the effect of randomization on various network properties. Specifically, authors highlighted on the spectrum because the eigen values of a network are closely associated to many important topological characteristics. They also conducted extensive experiments to achieve edge anonymity. The authors also proposed and carried out an empirical evaluation on spectrum preserving graph randomization method, which better preserve network properties thereby conserving edge anonymity. This edge editing approach for protecting graph privacy may largely demolish the properties of a graph. The edge editing method sometimes may modify the distance properties considerably by connecting two distant nodes together.

Also mining over these data might lead to erroneous conclusion about how the salaries are distributed in the society. Hence, exclusively relying on edge editing may not always be a solution to preserve data utility. Another

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 1, Issue 8, October 2013

novel idea is proposed by Mingxuan Yuan, Lei Chen et.al., (2013) [35] to preserve important graph properties, such as distances between nodes by appending some "noise" nodes into a graph. The core idea behind this is that many social networks satisfy the Power Law distribution [2], i.e., there exist a huge number of low degree vertices in the graph which could be used to hide appended noise nodes from being reidentified. Some graph nodes could be preserved much better by appending noise nodes than the existing pure edge-editing method.

E.M. Knorr, R.T. Ng, and V. Tucakov (2000)[16] dealt with finding outliers [14] in large, multidimensional datasets. The identification of outliers can lead to the discovery of truly unexpected knowledge in areas such as e-commerce, credit card frauds, and even drug analysis of performance informational statistics of athletes. Existing methods for finding outliers in large datasets can only deal efficientlywith two dimensions/attributes of a dataset. Authors, study the notion of DB- (Distance- Based) outliers and provide a proper and experimental evidence showing the value of DB-outliers, and focused on the development of algorithms for computing such outliers. Firstly, authors presented two simple algorithms, both having a complexity of O(k N2), k being the dimensionality and N being the number of objects in the dataset. These algorithms readily support datasets with more than two attributes. Secondly, an optimized cell-based algorithm is presented that has a complexity that is linear with respect to N, but exponential with respect to k. Thirdly, for datasets that are mainly disk-resident, authors present another version of the cell-based algorithm that guarantees at most 3 passes over a dataset and provide experimental results showing that these cellbased algorithms are by far the best for k<= 4.

G. Ghinita, P. Karras, P. Kalnis, and N. Mamoulis (2007) [12] and G. Ghinita, P. Karras, P. Kalnis, and N. Mamoulis (2009) [13] designed heuristic algorithms for single dimensional l-diversity models that do not exhibit k-anonymous requirement. G. Ghinita, P. Karras, P. Kalnis, and N. Mamoulis (2007) [12] [13] focused on one-dimensional quasi-identifiers, and studied the properties of optimal solutions for k-anonymity and l-diversity, based on sensible information loss metrics. Based on these properties, they develop efficient heuristics to solve the one-dimensional problems in linear time. Also the authors generalized the generated solutions to multi-dimensional quasi-identifiers using space-mapping techniques which outperforms other methods in literature in terms of execution time and information loss.

K.P. Puttaswamy, A. Sala, and B.Y. Zhao (2009) [24] analyzed the status of privacy protection in social content-sharing applications and described effective privacy attacks against today's social networks, and proposed anonymization techniques to protect users. Authors proved that simple protection mechanisms such as anonymizing shared data can still leave users open to "social intersection attacks", where certain of compromised users can identify the originators of shared content. By formulating this as a graph anonymization problem, authors propose to provide users with k-anonymity privacy guarantees by supplementing the social graph with "latent edges." They inventied StarClique, a locally minimal graph structure required for users to attain k-anonymity, where at worst, a user is identified as one of k possible contributors of a data object.

V. CONCLUSION AND FUTURE WORK

In this study, extensive work done currently on privacy preserving databases is reported. Several approaches of anonymization and knowledge hiding have been studied and the results were observed. Algorithms pertaining to ensuring database privacy have been studied along with the computation overhead involved in implementing the algorithms for real and synthetic data sets. Several methods of ensuring privacy such as k-anonymity and its variants were systematically analyzed. Despite the k-anonymity model, an intruder may gain access the sensitive information if a set of nodes share similar attributes. Also we make a detailed study on k-degree-l-diversity anonymity model, which takes into consideration the structural information and sensitive labels of individuals as well. Also the study the algorithmic impact of adding noise nodes to original graph and the rigorous analyses on the theoretical limitations of the appended noise nodes and its impact. In future we planned to enhance the algorithm for significant improvement in terms of algorithm efficiency, percentage of noise nodes and in terms of several other metrics. This survey would promote a lot of research directions in the field of social networking database privacy through anonymization

REFERENCES

[1] L. Backstrom, C. Dwork, and J.M. Kleinberg, "Wherefore Art Thou r3579x?: Anonymized Social Networks, Hidden Patterns, and Structural Steganography," Proc. Int'l Conf. World Wide Web (WWW), pp. 181-190, 2007.
[2] A.-L. Baraba´si and R. Albert, "Emergence of Scaling in Random Networks," Science, vol. 286, pp. 509-512, 1999.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 1, Issue 8, October 2013

[3] S. Bhagat, G. Cormode, B. Krishnamurthy, and D. Srivastava, "Class-Based Graph Anonymization for Social Network Data," Proc. VLDB Endowment, vol. 2, pp. 766-777, 2009.
[4] A. Campan and T.M. Truta, "A Clustering Approach for Data and Structural Anonymity in Social Networks," Proc. Second ACM SIGKDD Int'l Workshop Privacy, Security, and Trust in KDD (PinKDD '08), 2008.
[5] A. Campan, T.M. Truta, and N. Cooper, "P-Sensitive K-Anonymity with Generalization Constraints," Trans. Data Privacy, vol. 2, pp. 65-89, 2010.
[6] J. Cheng, A.W.-c. Fu, and J. Liu, "K-Isomorphism: Privacy Preserving Network Publication against Structural Attacks," Proc. Int'l Conf. Management of Data, pp. 459-470, 2010.
[7] G. Cormode, D. Srivastava, T. Yu, and Q. Zhang, "Anonymizing Bipartite Graph Data Using Safe Groupings," Proc. VLDB Endowment, vol. 1, pp. 833-844, 2008.
[8] S. Das, O. Egecioglu, and A.E. Abbadi, "Privacy Preserving in Weighted Social Network," Proc. Int'l Conf. Data Eng. (ICDE '10), pp. 904-907, 2010.
[9] W. Eberle and L. Holder, "Discovering Structural Anomalies in Graph-Based Data," Proc. IEEE Seventh Int'l Conf. Data Mining Workshops (ICDM '07), pp. 393-398, 2007.
[10] K.B. Frikken and P. Golle, "Private Social Network Analysis: How to Assemble Pieces of a Graph Privately," Proc. Fifth ACM Workshop Privacy in Electronic Soc. (WPES '06), pp. 89-98, 2006.
[11] S.R. Ganta, S. Kasiviswanathan, and A. Smith, "Composition Attacks and Auxiliary Information in Data Privacy," Proc. ACM SIGKDD Int'l Conf. Knowledge Discovery and Data Mining, pp. 265- 273, 2008.
[12] G. Ghinita, P. Karras, P. Kalnis, and N. Mamoulis, "Fast Data Anonymization with Low Information Loss," Proc. 33rd Int'l Conf. Very Large Data Bases (VLDB '07), pp. 758-769, 2007.
[13] G. Ghinita, P. Karras, P. Kalnis, and N. Mamoulis, "A Framework for Efficient Data Anonymization Under Privacy and Accuracy Constraints," ACM Trans. Database Systems, vol. 34, pp. 9:1-9:47, July 2009.
[14] J. Han, Data Mining: Concepts and Techniques. Morgan Kaufmann Publishers, Inc., 2005.
[15] M. Hay, G. Miklau, D. Jensen, D. Towsley, and P. Weis, "Resisting Structural Re-Identification in Anonymized Social Networks," Proc. VLDB Endowment, vol. 1, pp. 102-114, 2008.
[16] E.M. Knorr, R.T. Ng, and V. Tucakov, "Distance-Based Outliers: Algorithms and Applications," The VLDB J., vol. 8, pp. 237-253, Feb. 2000.
[17] N. Li and T. Li, "T-Closeness: Privacy Beyond K-Anonymity and L-Diversity," Proc. IEEE 23rd Int'l Conf. Data Eng. (ICDE '07), pp. 106-115, 2007.
[18] K. Liu and E. Terzi, "Towards Identity Anonymization on Graphs," SIGMOD '08: Proc. ACM SIGMOD Int'l Conf. Management of Data, pp. 93-106, 2008.
[19] L. Liu, J. Wang, J. Liu, and J. Zhang, "Privacy Preserving in Social Networks against Sensitive Edge Disclosure," Technical Report CMIDA-HiPSCCS 006-08, 2008.
[20] A. Machanavajjhala, D. Kifer, J. Gehrke, and M.Venkitasubramaniam, "L-Diversity: Privacy Beyond K-Anonymity," ACM Trans. Knowledge Discovery Data, vol. 1, article 3, Mar. 2007.
[21] A. Narayanan and V. Shmatikov, "De-Anonymizing Social Networks," Proc. IEEE 30th Symp. Security and Privacy, pp. 173-187, 2009.
[22] C.C. Noble and D.J. Cook, "Graph-Based Anomaly Detection," Proc. Ninth ACM SIGKDD Int'l Conf. Knowledge Discovery and Data Mining (KDD '03), pp. 631-636, 2003.
[23] L. Page, S. Brin, R. Motwani, and T. Winograd, "The Pagerank Citation Ranking: Bringing Order to the Web," Proc. World Wide Web Conf. Series, 1998.
[24] K.P. Puttaswamy, A. Sala, and B.Y. Zhao, "Starclique: Guaranteeing User Privacy in Social Networks Against Intersection Attacks," Proc. Fifth Int'l Conf. Emerging Networking Experiments and Technologies (CoNEXT '09), pp. 157-168, 2009.
[25] N. Shrivastava, A. Majumder, and R. Rastogi, "Mining (Social) Network Graphs to Detect Random Link Attacks," Proc. IEEE 24th Int'l Conf. Data Eng. (ICDE '08), pp. 486-495, 2008.
[26] L. Sweeney, "K-Anonymity: A Model for Protecting Privacy," Int'l J. Uncertain. Fuzziness Knowledge-Based Systems, vol. 10, pp. 557- 570, 2002.
[27] X. Xiao and Y. Tao, "Anatomy: Simple and Effective Privacy Preservation," Proc. 32nd Int'l Conf. Very Large Databases (VLDB '06), pp. 139-150, 2006.
[28] X. Ying, X. Wu, and D. Barbara, "Spectrum Based Fraud Detection in Social Networks," Proc. IEEE 27th Int'l Conf. Very Large Databases (VLDB '11), 2011.
[29] X. Ying and X. Wu, "Randomizing Social Networks: A Spectrum Preserving Approach," Proc. Eighth SIAM Conf. Data Mining (SDM'08), 2008.
[30] E. Zheleva and L. Getoor, "Preserving the Privacy of Sensitive Relationships in Graph Data," Proc. First SIGKDD Int'l Workshop Privacy, Security, and Trust in KDD (PinKDD '07), pp. 153-171, 2007.
[31] E. Zheleva and L. Getoor, "To Join or Not to Join: The Illusion of Privacy in Social Networks with Mixed Public and Private User Profiles," Proc. 18th Int'l Conf. World Wide Web (WWW '09), pp. 531-540, 2009.
[32] B. Zhou and J. Pei, "Preserving Privacy in Social Networks Against Neighborhood Attacks," Proc. IEEE 24th Int'l Conf. Data Eng. (ICDE '08), pp. 506-515, 2008.
[33] B. Zhou and J. Pei, "The K-Anonymity and L-Diversity Approaches for Privacy Preservation in Social Networks against Neighborhood Attacks," Knowledge and Information Systems, vol. 28, pp. 47-77, 2011.
[34] L. Zou, L. Chen, and M.T. O¨zsu, "K-Automorphism: A General Framework for Privacy Preserving Network Publication," Proc. VLDB Endowment, vol. 2, pp. 946-957, 2009.
[35] Mingxuan Yuan, Lei Chen, Philip S. Yu, Ting Yu, "Protecting Sensitive Labels in Social Network Data Anonymization", IEEE Transactions on Knowledge and Data Engineering, Vol. 25, No. 3, pp.633-647, March 2013
[36] S.Balamurugan, P.Visalakshi, "Modified Partitioning Algorithm for Privacy Preservation in Microdata Publishing with Full Functional Dependencies", Australian Journal of Basic and Applied Sciences, 7(8): pp.316-323, July 2013

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 1, Issue 8, October 2013

BIOGRAPHY

S.Charanyaa obtained her B.Tech degree in Information Technology from Bannari Amman Institute of Technology, Sathyamangalam, Tamil Nadu, India. She is currently pursuing her M.Tech degree in Information Technology at S.N.S. College of Technology, Coimbatore, Tamilnadu, India. Her areas of research interest accumulate in the areas of Database Security, Privacy Preserving Database, Object Modeling Techniques, and Software Engineering.

Prof.T.Shanmugapriya is currently working as Assistant Professor in the Department of Information Technology at S.N.S. College of Technology, Coimbatore, Tamilnadu, India. She has 6 years and 2 months of teaching experience. She has published a number of research papers which include 4 International Journals, 5 National Conferences and 3 International Conferences. Her areas of research interest accumulate in the area of Computer Networks.