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. 2, Issue 3, March 2014

Proposing a Novel Synergized K-Degree L-Diversity T-Closeness Model for Graph Based Data Anonymization

S.Charanyaa[1], K.Sangeetha[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: Privacy becoming a major concern in publishing sensitive information of the individuals in the social network data. A lot of anonymization techniques are evolved to protect sensitive information of individuals. k-anonymity is one of the data anonymization framework for protecting privacy that emphasizes the lemma, every tuple should be different from at least k-1 other tuples in accordance with their quasi-identifiers(QIDs). Researchers have developed privacy models similar to k-anonymity but still label-node relationship is not well protected. In this paper, we propose a novel synergized k-degree l-diversity t-closeness model to effectively anonymize graphical data at marginal information loss, thereby controlling the distribution of sensitive information in graphical structure based on the threshold value. Experimental evidences indicate the substantial reduction in information loss ratio during synergy.

Keywords: Data Anonymization, Graphical Data, Sensitive information, k-anonymity, l-diversity, t-closeness

I. INTRODUCTION

The collection of digital information by governments, corporations, and individuals has created tremendous opportunities for knowledge-based decision making. Driven by mutual benefits, or by regulations that require certain data to be published, there is a demand for the exchange and publication of data among various parties. For example, licensed hospitals in California are required to submit specific demographic data on every patient discharged from their facility**.** Detailed person-specific data in its original form often contains sensitive information about individuals, and publishing such data immediately violates individual privacy. The current practice primarily relies on policies and guidelines to restrict the types of publishable data and on agreements on the use and storage of sensitive data. The limitation of this approach is that it either distorts data excessively or requires a trust level that is impractically high in many data-sharing scenarios. For example, contracts and agreements cannot guarantee that sensitive data will not be carelessly misplaced and end up in the wrong hands. A task of the utmost importance is to develop methods and tools for publishing data in a more hostile environment, so that the published data remains practically useful while individual privacy is preserved. This undertaking is called privacy-preserving data publishing (PPDP). In the past few years, research communities have responded to this challenge and proposed many approaches. While the research field is still rapidly developing, it is a good time to discuss the assumptions and desirable properties for PPDP, clarify the differences and requirements that distinguish PPDP from other related problems, and systematically summarize and evaluate different approaches to PPDP.

The rest of the paper is organized as follows. Section 2 describes the anonymization scenario. A detailed literary review is presented in Section 3. Section 4 describes the steps involved in KDLDTC model creation. The detailed construction mechanism of KDLDTC model is discussed in Section 5. Section 6 describes about the experimental results and discussions. Section 7 concludes the paper and outlines the direction for future work.

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. 2, Issue 3, March 2014

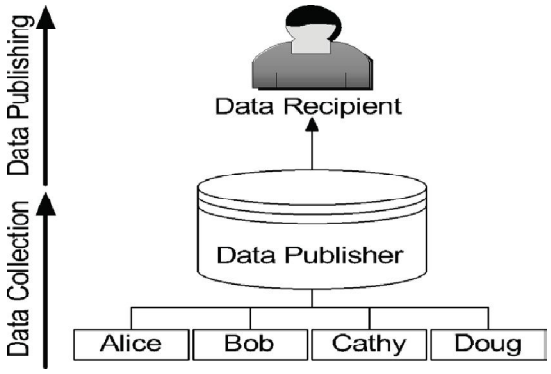

Fig.1. A two-phase data anonymization and publishing model

II. ANONYMIZATION SCENARIO

The world is experiencing lot of data collections containing metadata and disk storage apace become increasingly affordable. Metadata is defined as person specific data i.e., information related to one particular person, household or an organization. To protect privacy for these data collections, data anonymization is used. Data anonymization is defined as replacing the contents of identifiable fields in a database

In the most basic form of privacy-preserving data publishing (PPDP) [3], the data holder has a table of the form: D (Explicit Identifier, Quasi Identifier, Sensitive Attributes, non-Sensitive Attributes), where Explicit Identifier is a set of attributes, such as name and social security number SSN), containing information that explicitly identifies record owners, Quasi Identifier is a set of attributes that could potentially identify record owners, Sensitive Attributes consist of sensitive person-specific information such as disease, salary, and disability status and Non-Sensitive Attributes contains all attributes that do not fall into the previous three categories

Privacy preserving publishing of microdata has been studied extensively in recent years. Microdata contain records each of which contains information about an individual entity, such as a person, a household, or an organization. Several microdata anonymization techniques have been proposed. The most popular ones are generalization, for k-anonymity and bucketization for diversity. In both approaches, attributes are partitioned into three categories:

- Some attributes are identifiers that can uniquely identify an individual, such as Name or Social Security Number.
- Some attributes are Quasi Identifiers (QI), which the adversary may already know (possibly from other publicly available databases) and which, when taken together, can potentially identify an individual, e.g., Birthdate, Sex, and Zipcode.
- Some attributes are Sensitive Attributes (SAs), which are unknown to the adversary and are considered sensitive, such as Disease and Salary.

It has been shown [1-3] that generalization for k- anonymity losses considerable amount of information, especially for high-dimensional data. This is due to the following three reasons. First, generalization for k-anonymity suffers from the curse of dimensionality. In order for generalization to be effective, records in the same bucket must be close to each other so that generalizing the records would not lose too much information. However, in high-dimensional data, most data points have similar distances with each other, forcing a great amount of generalization to satisfy k-anonymity even for relative small k's.

Second, in order to perform data analysis or data mining tasks on the generalized table, the data analyst has to make the uniform distribution assumption that every value in a generalized interval/set is equally possible, as no other distribution assumption can be justi- fied. This significantly reduces the data utility of the generalized data. Third, because each attribute is generalized separately, correlations between different attributes are lost. In order to study attribute correlations on the generalized table, the data analyst has to assume that every possible combination of attribute values is equally possible. This is an inherent problem of generalization that prevents effective analysis of attribute correlations.

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. 2, Issue 3, March 2014

Novel data anonymization technique called slicing to improve the current state of the art. Slicing partitions the dataset both vertically and horizontally. Vertical partitioning is done by grouping attributes into columns based on the correlations among the attributes. Each column contains a subset of attributes that are highly correlated. Horizontal partitioning is done by grouping tuples into buckets. Finally, within each bucket, values in each column are randomly permutated (or sorted) to break the linking between different columns.

The basic idea of slicing is to break the association cross columns, but to preserve the association within each column. This reduces the dimensionality of the data and preserves better utility than generalization and bucketization. Slicing preserves utility because it groups highly-correlated attributes together, and preserves the correlations between such attributes. Slicing protects privacy because it breaks the associations between uncorrelated attributes, which are infrequent and thus identifying. Note that when the dataset contains QIs and one SA, bucketization has to break their correlation; slicing, on the other hand, can group some QI attributes with the SA, preserving attribute correlations with the sensitive attribute.

III. LITERARY REVIEW

The main disadvantage of Generalization is: it loses considerable amount of information, especially for high-dimensional data. And also, Bucketization does not prevent membership disclosure and does not apply for data that do not have a clear separation between quasi-identifying attributes and sensitive attributes. Generalization loses considerable amount of information, especially for high- dimensional data. Bucketizations do not have a clear separation between quasi-identifying attributes and sensitive attributes.

K-anonymity has been well adopted; Machanavajjhala *et al*. [4] showed that a *k*-anonymous table may still have some subtle but severe privacy problems due to the lack of diversity in the sensitive attributes. In particular, they showed that, the degree of privacy protection does not really depend on the size of the equivalence classes on quasi-identifier attributes which contain tuples that are identi- cal on those attributes. Instead, it is determined by the number and distribution of distinct sensitive values associ- ated with each equivalence class. To overcome the weakness in *k*-anonymity, they propose the notion of *l*-diversity [4].

Xiao and Tao [5] prove that *l*-diversity always guarantees stronger privacy preservation than *k*-anonymity. Though several important models and many efficient algorithms have been proposed to preserve privacy in relational data, most of the existing studies can deal with relational data only. Those methods cannot be applied to social network data straightforwardly. Anonymizing social network data is much more challenging than anonymizing relational data [6]. First, it is much more challenging to model background knowledge of adversaries and attacks about social network data than that about relational data. On relational data, it is often assumed that a set of attributes serving as a quasi-identifier is used to associate data from multiple tables, and attacks mainly come from identifying individuals from the quasi-identifier. However, in a social network, many pieces of information can be used to identify individuals, such as labels of vertices and edges, neighborhood graphs, induced subgraphs, and their combinations. It is much more com-plicated and much more difficult than the relational case. Second, it is much more challenging to measure the information loss in anonymizing social network data than that in anonymizing relational data. Typically, the information loss in an anonymized table can be measured using the sum of information loss in individual tuples. Given one tuple in the original table and the corresponding anonymized tuple in the released table, we can calculate the distance between the two tuples to measure the information loss at the tuple level. However, a social network consists of a set of vertices and a set of edges. It is hard to compare two social networks by comparing the vertices and edges individually. Two so- cial networks having the same number of vertices and the same number of edges may have very different network-wise properties such as connectivity, betweenness, and diameter. Thus, there can be many different ways to assess information loss and anonymization quality.

Liu et al. [7] and Zheleva and Getoor [5] proposed a catgorization schema di®erent from ours in this paper. They classified privacy in social networks into identity disclosure(that is, the identity of an individual who is associated with a vertex is revealed), link disclosure (that is, the sensitive relationship between two individuals is disclosed), and content disclosure (that is, the sensitive data associated with each vertex is compromised, for example, the email messages sent and/or received by the individuals in an email communica-tion network). The categorization presented here is more extensive than the three categories in [5,7].

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. 2, Issue 3, March 2014

IV. K-DEGREE L-DIVERSITY T-CLOSENESS MODEL CREATION

A micro data table contains the details of an individual with sensitive informations that needs to be anonymized before the data is published in the social network. The initial table is anonymized by applying k-degree anonymization technique in which every tuple should be different from at least k-1 other tuples in accordance with their quasi-identifiers (QIDs). K-degree anonymity is used to preserve structure attack. K-degree alone is not sufficient to preserve node-label relationship in the graphical data. As a result l-diversity is employed to provide diversification in the equivalence class. L-diversity [4] in a literature says, there exists at least l distinct labels in each equivalence class. K-degree l-diversity anonymized table includes more information loss.

In this paper, along with k-degree l-diversity t-closeness is employed, which requires that the distribution of a sensitive attribute in any equivalence class is close to the distribution of the attribute in the overall table (i.e., the distance between the two distributions should be no more than a threshold t), and k degree. Combine k-degree anonymity with t- closeness to prevent not only the reidentification of individual nodes but also the revelation of a sensitive attribute associated with each node. In this work use distinct t-closeness to demonstrate our algorithm and give the detailed discussion about how more complex recursive (c,t) can be implemented. We propose a novel graph construction technique which makes use of noise nodes to preserve utilities of the original graph. Two key properties are considered:

1) Add as few noise edges as possible
2) Change the distance between nodes as less as possible.

We present analytical results to show the relationship between the number of noise nodes added and their impacts on an important graph property.

We also propose a novel privacy notion called t-closeness with k degree model, which requires that the distribution of a sensitive attribute in any equivalence class is close to the distribution of the attribute in the overall table (i.e., the distance between the two distributions should be no more than a threshold t), and k degree. A graph is k-degree anonymous if and only if for any node in this graph, there exist at least k - 1 other nodes with the same degree along with t threshold to satisfy and also additionally add the calculation of information loss ratio for t-closeness function. We choose the Earth Mover Distance to measure t-closeness requirement. This effectively limits the amount of individual-specific information an observer can learn. Further, in order to incorporate distances between values of sensitive attributes, we use the Earth Mover Distance metric.

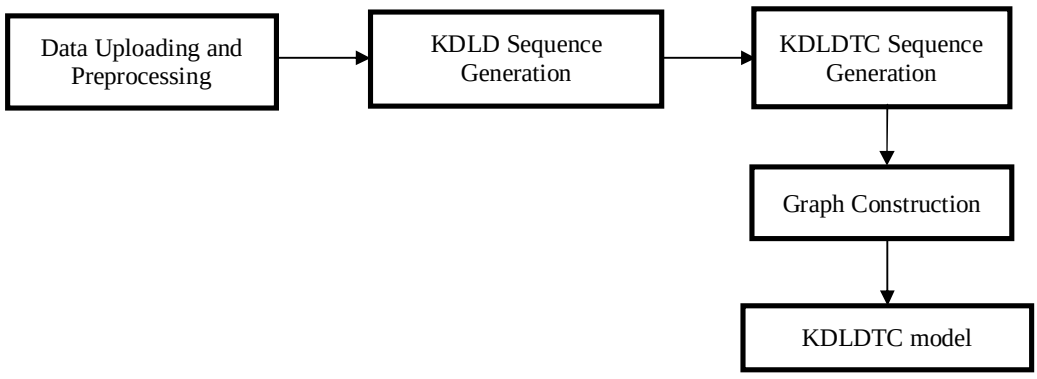

Fig 2. Sequence of steps involved in KDLDTC model generation

V. KDLDTC MODEL CONSTRUCTION

KDLDTC model is a combination of three models, k-degree, l-diversity and t-closeness principles of data anonymization adapted for graphical data model. K-degree L-diversity prevents node reidentification and also exposes label for each node when publishing. T-closeness an another model of data anonymization is combined with KDLD to prevent information loss by using Earth movers distance calculation method. By using the anonymized data, social network i.e., graph is constructed by adding noise nodes to create perplex among the intruders. In KDLDTC model the nodes in the graph are distributed based on the threshold value (the distribution of a sensitive attribute in any

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. 2, Issue 3, March 2014

equivalence class is close to the distribution of the attribute in the overall table i.e., the distance between the two distributions should be no more than a threshold t), by using Earth movers distance calculation.

A. Data Uploading and Pre-processing

Metadata from the real dataset is loaded into the execution environment. The loaded dataset needs to be pre-processed by the pre-processing module. The module truncates the most unwanted symbols from the dataset. Pre-processed dataset needs to be used for anonymizing

B. KDLD Sequence Generation

KDLD sequence is generated by combining k-anonymity and l-diversity anonymization techniques. The preprocessed metadata is k – degree anonymized in which every tuple should be different from at least k-1 other tuples in accordance with their quasi-identifiers (QIDs). The k-anonymized dataset is again anonymized by applying l-diversity technique to provide diversification in the equivalence class.

C. KDLDTC Sequence Generation

Metadata is preprocessed and is anonymized using k-degree and l-diversity. T-closeness is another anonymization technique in which distribution of a sensitive attribute in any equivalence class is close to the distribution of the attribute in the overall table (i.e., the distance between the two distributions should be no more than a threshold t), and k degree. Nodes in the social network graph is distributed based on the threshold value. Threshold value is calculated using Earth movers distance method [12]. The degree sequence of the initial social network graph is considered as P. Once the data is anonymized, a new degree sequence P^{new}.is created by using KDLDTC sequence generation algorithm. The nodes with the similar degrees are grouped together by using two cost factors namely C_{new} and $C_{merge.}$ where C_{new} is the cost of creating new group and C_{merge} is the cost of merging the node to the same group. Finally mean degree change of each node is calculated and target degree is fixed.

Given an unprocessed input dataset D; cost C_{new} and C_{merge}, term frequency T_{tf}, the term frequency entropy based KDLDTC sequence generation algorithm that will create a sequence P_{new} with minimal distortion is given below:

Algorithm 1: Term Frequency Entropy Based KDLDTC Sequence Generation Algorithm
Input: An unprocessed input dataset D; cost C_{new} and C_{merge} term frequency T_{tf}
1. Preprocess (D);
2. **Repeat** until no tuple is ungrouped
3. **Repeat** for each tuple
4. **Calculate** threshold (t), Entropy(e)
5. **Group** Dataset -> $G_1,G_2,...,G_{n-1}$, G_n w.r.t. term frequency T_{tf} **;**
6. **cluster: Form Cluster** on the basis of cost value C_{new} and C_{merge};
7. **Repeat** for all nodes
8. Calculate Degree(Node);
9. Calculate Mean_Degree(AllNodes);
10. goto cluster;

Finally a new KDLDTC sequence (P_{new}) will be created based on term frequency of tuples with least distortion of each nodes.

D. Graph Construction

Graph is constructed based on the new KDLDTC sequence generation (P^{new}). Graph construction module includes the following steps.

1) Neighborhood Edge Editing: It is the concept of adding new edges between the nodes. Neighborhood rule is followed in this approach i.e., to add edge between two neighbors, so that the path the nodes would be short as possible

2) Adding Node Decrease Degree: For any node whose degree is larger than its target degree in P^{new}, then decrease its degree to the target degree by making using of noise nodes

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. 2, Issue 3, March 2014

3) Adding Node Increase Degree: For any node whose degree is smaller than its target degree in P^{new}, then increase its degree to the target degree by making using of noise nodes
4) New Node Degree Setting: For any noise node, if its degree does not appear in Pnew, does some adjustment to make it has a degree in Pnew. Then, the noise nodes are added into the same degree groups in Pnew;
5) New Node Label Setting: In this step assign sensitive labels to noise nodes to make sure all the same degree groups still satisfy the requirement of the distinct l and t –closeness. In each same degree group, there are already l distinct and t-closeness sensitive labels in it, it is obviously the new added noise nodes can have any sensitive label.

VI. RESULTS AND DISCUSSIONS

A proposed method to preserve important graph properties, such as distances between nodes by adding certain "noise" nodes into a graph. In proposed system, privacy preserving is to prevent an attacker from reidentifying a user and finding the fact that a certain user has a specific sensitive value. To achieve this goal, k-degree-l-diversity model is proposed for safely publishing a labeled graph, and then develop corresponding graph anonymization algorithms with the least distortion to the properties of the original graph, such as degrees and distances between nodes. K-degree anonymity with l-diversity is combined to prevent not only the reidentification of individual nodes but also the revelation of a sensitive attribute associated with each node. Further entropy based t-closeness mechanism is employed to achieve reduced information loss. The algorithm is implemented and tested in a Dell Laptop with Intel Core i5 Pentium IV CPU with 6 GB RAM and 64-bit Windows XP OS. The algorithm is implemented in Netbeans IDE 6.9.1 with MySQL as backend.

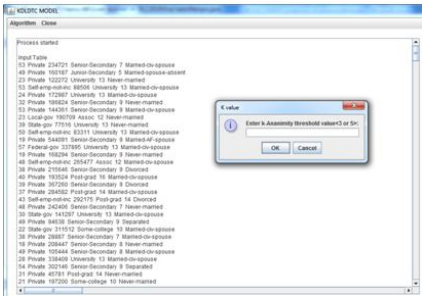

Fig 3. Initial microdata table- fixing the k-degree for anonymization

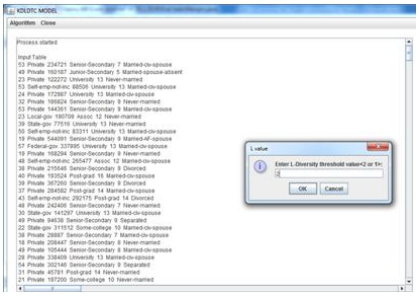

Fig 4. Fixing l-diversity for anonymization after fixing k-degree

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. 2, Issue 3, March 2014

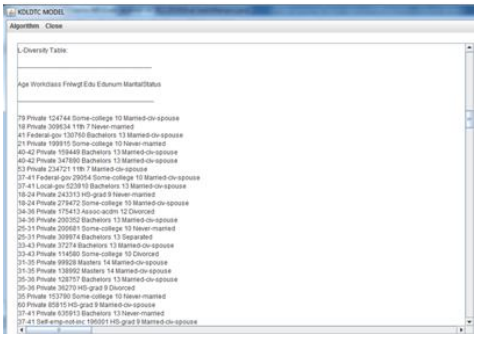

Fig 5. K-Degree L-Diversified Microdata table

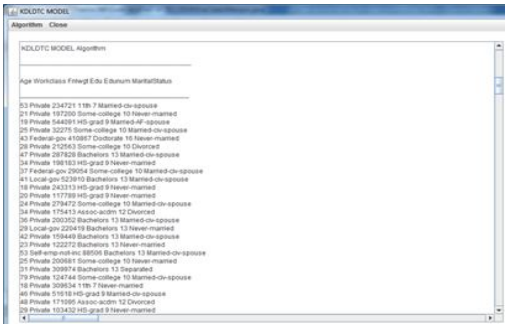

Fig 6. Anonymized Microdata after implementing KDLDTC algorithm

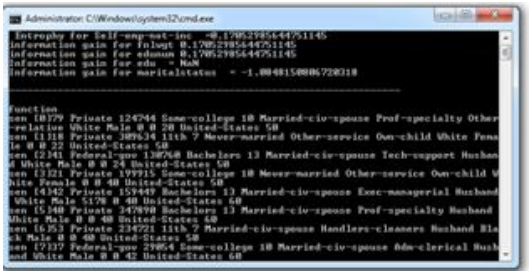

Fig 7. Entropy and Information Gain for each value in Anonymized Microdata table

The entropy calculation for each value of sensitive attributes of the KDLDTC anonymized microdata table is done using the following Java code snippet

```
double entrophycal(double p,double n)
        {double ent;
        double pos,neg;
        pos=p/(p+n);
        neg=n/(p+n);
        ent=-pos*Math.log(pos)-neg*Math.log(neg);
        return ent; }
```

VII. CONCLUSION AND FUTURE WORK

A novel methodology of k-degree l-diversity t-closeness model for privacy preserving social network data is implemented. In order to achieve the requirement of k-degree-l-diversity-t-closeness design a noise node adding algorithm is employed to construct a new graph from the original graph with a restriction of introducing minimal distortions to the original graph. It gives rigorous analysis of the theoretical bounds on the number of noise nodes added

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. 2, Issue 3, March 2014

and their impacts on an important graph property. Our extensive experimental results demonstrate the reduced information loss incurred in synergizing k-degree l-diversity and t-closeness mechanisms. In future, we have plans to develop algorithms which can reduce the number of noise nodes if the noise nodes contribute to both anonymization and diversity. Another interesting direction is to consider how to implement this protection model in a distributed environment, where different publishers publish their data independently and their data are overlapping. In a distributed environment, although the data published by each publisher satisfy certain privacy requirements, an attacker can still break user's privacy by combining the data published by different publishers.

REFERENCES

[1] C. Aggarwal. On k-anonymity and the curse of dimensionality. In VLDB, pages 901–909, 2005.

[2] B.-C. Chen, R. Ramakrishnan, K. LeFevre. Privacy skyline: Privacy with multidimensional adversarial knowledge. In VLDB, pages 770–781, 2007.

[3] X. Xiao and Y. Tao. Anatomy: simple and effective privacy preservation. In VLDB, pages 139–150, 2006.

[4] A. Machanavajjhala, J. Gehrke, D. Kifer, and M. Venkitasubramaniam. L-diversity: Privacy beyond k-anonymity. In Proceedings of the 22nd IEEE International Conference on Data Engineering (ICDE'06), Washington, DC, USA, 2006. IEEE Computer Society

[5] X. Xiao and Y. Tao. Personalized privacy preservation. In Proceedings of the 2006 ACM SIGMOD international conference on Management of data (SIG- MOD'06), pages 229-240, New York, NY, USA, 2006.ACM Press.

[6] B. Zhou and J. Pei. Preserving privacy in social networks against neighborhood attacks. In Proceedings of the 24th IEEE International Conference on Data Engineering (ICDE'08), pages 506-515, Cancun, Mexico, 2008. IEEE Computer Society.

[7] K. Liu, K. Das, T. Grandison, and H. Kargupta. Privacy-preserving data analysis on graphs and social networks. In H. Kargupta, J. Han, P. Yu, R. Motwani, and V. Kumar, editors, Next Generation Data Mining. CRC Press, 2008.

[8] M. Hay, G. Miklau, D. Jensen, and D. Towsley. Resistng structural identification in anonymized social net- works. In Proceedings of the 34th International Conference on Very Large Databases (VLDB'08). ACM, 2008.

[9] S. J. Russell and P. Norvig. Artificial Intelligence: A Modern Approach. Pearson Education, 2003.

[10] A. Campan and T. M. Truta. A clustering approach for data and structural anonymity in social networks. In Proceedings of the 2nd ACM SIGKDD International Workshop on Privacy, Security, and Trust in KDD (PinKDD'08), , Las Ve- gas, Nevada, USA, 2008.

[11] L. Sweeney, "K-Anonymity: A Model for Protecting Privacy," Int'l J. Uncertain. Fuzziness Knowledge-Based Systems, vol. 10, pp. 557-570, 2002.

[12] 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.

[13] 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.

[14] 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.

[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] 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.

[17] 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.

[18] 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.

[19] 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.

[20] X. Ying and X. Wu, "Randomizing Social Networks: A Spectrum Preserving Approach," Proc. Eighth SIAM Conf. Data Mining, 2008.

[21] 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

[22] 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

[23] S.Charanyaa, T.Shanmugapriya, "Certain Investigations on Approaches for Protecting Graph Privacy in Data Anonymization", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 1, Issue 8, October 2013

[24] S.Charanyaa, T.Shanmugapriya, "A Survey on Attack Prevention and Handling Strategies in Graph Based Data Anonymization" International Journal of Advanced Research in Computer and Communication Engineering, Vol. 2, Issue 10, October 2013.

[25] S.Charanyaa, K.Sangeetha,"Term Frequency Based Sequence Generation Algorithm for Graph Based Data Anonymization ", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 2, Issue 2, February 2014.

[26] S.Charanyaa, K.Sangeetha," Strategies for Knowledge Based Attack Detection in Graphical Data Anonymization", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 3, Issue 2, February 2014.

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. 2, Issue 3, March 2014

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. She has published 4 International Journals in the research domain of Database Privacy. Her areas of research interest accumulate in the areas of Database Security, Privacy Preserving Database, Object Modeling Techniques, and Software Engineering.

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