DOI: 10.21917/ijsc.2016.0189

PRIVACY PRESERVING DATA MINING USING MULTIPLE OBJECTIVE OPTIMIZATION

V. Shyamala Susan[1] and T. Christopher[2]
[1]*Department of Computer Science, Government Arts College, Udumalpet, India*
E-mail: [1]shyamalasusan@gmail.com
[2]*Department of Computer Science, Government Arts College, Coimbatore, India*
E-mail: [2]chris.hodcs@gmail.com

Abstract

Privacy preservation is that the most targeted issue in information publication, because the sensitive data shouldn't be leaked. For this sake, several privacy preservation data mining algorithms are proposed. In this work, feature selection using evolutionary algorithm and data masking coupled with slicing is treated as a multiple objective optimisation to preserve privacy. To start with, Genetic Algorithm (GA) is carried out over the datasets to perceive the sensitive attributes and prioritise the attributes for treatment as per their determined sensitive level. In the next phase, to distort the data, noise is added to the higher level sensitive value using Hybrid Data Transformation (HDT) method. In the following phase slicing algorithm groups the correlated attributes organized and by this means reduces the dimensionality by retaining the Advanced Clustering Algorithm (ACA). With the aim of getting the optimal dimensions of buckets, tuple segregating is accomplished by Metaheuristic Firefly Algorithm (MFA). The investigational consequences imply that the anticipated technique can reserve confidentiality and therefore the information utility is additionally high. Slicing algorithm allows the protection of association and usefulness in which effects in decreasing the information dimensionality and information loss. Performance analysis is created over OCC 7 and OCC 15 and our optimization method proves its effectiveness over two totally different datasets by showing 92.98% and 96.92% respectively.

Keywords:

Privacy Preservation, Genetic Algorithm, Advanced Clustering Algorithm, Metaheuristic Firefly Algorithm, Hybrid Data Transformation

1. INTRODUCTION

Data mining covenants by means of the technique of extracting helpful data from the databases and sorts this into helpful information. Data mining possesses many dimensions like text mining, web mining, information clumping, information organization and confidentiality protection etc. Confidentiality preservation is the utmost problem of research in information e-book and it offers practices for business organization to accumulate useful information. Typically the stages needed for doing the data mining obligations are information collection and information publication. In the information collection phase, the data handler gathers the data from the data possessor. The data publication department offers with the discharge of collected data to an information miner or to the information recipient. The information receiver excavates the available information. Confidentiality protection in information processing is sensitive, as a result of the individuality and different personal details mustn't be disclosed, despite the fact broadcasting information. But it must ensure data utility.

There exist three methods to acquire privacy preservation. They are perturbation, anonymization and cryptography [1]. The central theme of privacy preservation is to supply security to the sensitive data before publication. But in greater dimensional information set a whole ration of examination is necessary to separate the characteristics to Quasi Identifier (*QI*), sensitive attributes (*SA*) and non-sensitive (*NS*) attributes. Sometimes a characteristic may be entitled as in cooperation SA and QI which may perhaps result in troubles even as considering them with confidentiality practices. In this work, priority level of the sensitive attributes are diagnosed and labeled as high, medium or low based on the sensitive data vulnerability score. If the sensitive level of the data is high, it is identified as SA, and if they have mid- level they are identified as QI, actually small or no rank standards are measured as NS characteristics. If the sensitive level is higher, then there is higher the poor impact of any misuse of data. Hence higher sensitive level, the more potent techniques are needed to anonymise the data. Therefore, SA attributes are masked with three layered protection using HDT. The masked data are anonymised in addition using slicing algorithm to preserve confidentiality over horizontal and vertical segregating. In the vertical segregating stage, the pertinent characteristics are grouped with the aid of employing an ACA. In the succeeding stage the MFA accumulates the tuples into buckets in a horizontal way and guarantees l-diversity in every bucket. We have analyzed different data transformation methods like fuzzy C means, translation, rotation and scaling upon two different datasets. On analysis, we found that our multiple objective optimization algorithms outperform the others and produced better result in terms of accuracy, utility and privacy.

2. LITERATURE REVIEW

Privacy Preserving Data Mining (PPDM) is a promising research area that goes for averting security breaks which can happen while mining the information [1] [2] [3]. The motivation behind PPDM calculation is to change the first information, to look after protection that winds up in low level of information leakage. This may pave method for rendering smart mining results. Data anonymisation approaches preserves individual privacy using the methods such as k-anonymity using generalization [1]. These methods transform the dataset into k indistinguishable records from each other. Mostly, k-anonymity concept is employed by the PPDM algorithms so as to assure privacy [5]. But this method is not suitable for high dimensional data and to search out optimal k-anonymous datasets over generalization and is esteemed as NP-Hard [6] [7]. The work presented in [8] deals with a general taxonomy and number of other generalization schemes are compared. In [9], a genetic

framework is developed to look the simplest best set of generalization in order to satisfy k-anonymity constraints. So, every generalization is treated as a chromosome and this technique used very less memory and provided better results.

The work proposed in [10] provides security by a base up generalization theme. In [11], a generalization technique for classification by using K-anonymity is planned and it is a top down specialization algorithmic principle. This algorithmic rule is better than the base-up approach. In [12], the improvement to the algorithmic rule conferred in [11] is created. Several clustering techniques are proposed in [13] for generating domain hierarchies.

In [14], fuzzy logic is utilised to preserve sensitive information. At initially, the dataset is gathered and after that by employing a fuzzy membership utility, noise is added. A hybrid evolutionary algorithm using Genetic Algorithm and Particle Swarm Optimization (PSO) is proposed in [15]. The major drawback is that the PSO converges easily to a stable point. Genetic algorithms are significantly helpful in feature selection, while mining the data [16-18]. A genetic algorithm grounded structure is proposed in [19] to determine feature set segregating responsibilities. In [20], it is instructed that Genetic algorithms are useful particularly when the hunt space is massive. In this work, feature selection using evolutionary algorithm and data masking coupled with slicing is treated as a multiple objective optimization to preserve privacy.

3. PROPOSED WORK

First of all the GA is carried out over the dataset to discover the sensitive attributes and prioritise them for treatment as in line with their determined sensitive level. In the next phase, Hybrid Data Transformation function is used to feature noise to the higher level of sensitive values which releases distorted data. This is accompanied by applying slicing algorithm wherein vertical partition organizations the correlated attributes through using ACA. Tuple segregating is carried out via MFA to acquire the optimal dimensions of buckets. The experimental consequences imply that the proposed technique can maintain privacy of data, and thereby improves the information utility and accuracy. The architecture of the proposed work is as follows:

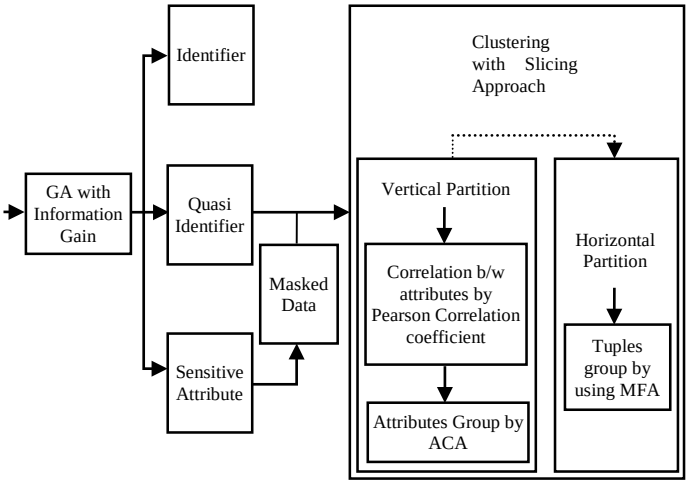

Fig.1. Proposed System Architecture

3.1 SENSITIVITY ANALYSIS PHASE BY GENETIC ALGORITHM

The search technique applied for sensitivity analysis is Genetic algorithm. The objective of this section is to pick out the priority level of the sensitive attributes. The sensitive level of the attributes can be labelled as high, medium or low. If the sensitive level is higher, then there may be better the poor impact of any misuse of data. Thus higher sensitive level, the stronger techniques are needed to anonymise the data.

The sensitive data vulnerability score for the attributes are identified as below.

Table.1. Sensitive data score

Sensitive Data Score	Sensitive level
≤ 4	High
Between 4 and 8	Medium
Between 8 and 12	Low

Genetic algorithm is an optimization algorithm employed for extracting the desirable features. The genetic operators powers up GA through selection, cross over and mutation. The initial population is created by using the formula

$$P = \sum_{i=1}^{N} I_i \tag{1}$$

where, I denote individuals. Fitness function is used to evaluate the individuals involved within the population. The fitness function of every individual is calculated, so as to choose an individual for reproduction.

$$f\left(S_i\right) = \sum_{j=1}^{m}\left(\frac{S_i\left(a_j\right)}{V_i\left(a_j\right)}\right) \tag{2}$$

$$V_i\left(a_j\right) = \sum_{j=1}^{n} S_i\left(a_j\right) \tag{3}$$

where, m is no. of attributes, n is no. of samples, $f(S_i)$ is fitness for a sample S_i and $V_i(a_j)$ is value of attribute a_j. Each newly generated population is evaluated by evaluation criteria.

The evaluation criteria employed for ranking is Information Gain, which calculates the probability of individual selection, on rank basis with respect to fitness values. Calculate the Information Gain (IG) by using,

$$IG\ (a_j) = \mathrm{E}\ (a_j) - \mathrm{E}\ (A_j) \tag{4}$$

$$E\left(a\right) = \sum_{j=1}^{m} a_j \log\left(a_j\right) \tag{5}$$

where, a_j is the ratio of conditional attribute a in dataset. When A_j has $|A_j|$ kinds of attribute values and condition attribute a_j partitions set a using attribute A_j, the value of information $E\ (A_j)$ is defined as,

$$E\left(A\right) = \sum_{j=1}^{m} A_j \log\left(A_j\right) \tag{6}$$

The individuals with high fitness values are selected as parents to produce offspring. Crossover is the next step. After crossover, mutation is the step that follows and the process is carried out with

the offspring. The following step outlines the Genetic algorithm with Information gain.

3.1.1 Genetic Algorithm with Information Gain:

Step 1: Create initial population of individuals

Step 2: Evaluate fitness for all individuals

Step 3: Rank the attributes based on Information Gain.

While (not termination)

{

Select fitter individuals;

Crossover;

Mutate the individuals;

1. Calculate the fitness of individuals;
2. If Attribute Rank Value ≥ Threshold Rank
   a. Then the value set attributes as *SA*
3. If Attribute Rank Value ≤ Threshold Rank Value
   a. Then project the Attributes as Low priority attributes and set as *QI* attribute of the dataset.
4. Generate new population;
5. Apply Hybrid Data transformation to *SA*

End while;

}

The higher sensitive values are masked by HDT method. The privacy is still improved by slicing algorithm. If the dataset's vulnerable score is low, then they are left unchanged.

3.2 HYBRID DATA TRANSFORMATION (HDT) METHOD

The process of data transformation method hides the sensitive information without loss of information and ensures the original dataset is equal to the distorted dataset. If the database consists of categorical data, it is transformed into binary attribute and mapped to numeric value. In the hybrid data transformation scheme, we select randomly one operation for each confidential attribute that can take the values {*Add, mult, Rotate*} in the set of operations. Thus, each confidential attribute is perturbed using an additive noise, multiplicative noise term followed by a rotation.

In the Translation Data Transformation Method, SA is masked through including noise. Similarly in the Scaling Data Transformation approach, *SA* attributes masked through the usage of multiplicative noise. In the Rotation Data Transformation Method noise is added in terms of usual rotation angle amongst the characteristics A_i and A_j. Contrasting the preceding approaches, Rotation Data Transformation may be functional added than when some intimate characteristics. Thus, every private characteristic is transformed using an additive, a multiplicative noise term, or a rotation. The outline of the algorithm is as follows:

3.2.1 HDT Algorithm:

Begin

Step 1: For each confidential attribute A_j in V

- Select the noise term $noise_j$ in N for the confidential attribute A_j
- The j-the operation $op_j \leftarrow$ {*Add*, *Mult*, *Rotation*}

Step 2: For each $v_i \in V$ do

For each a_j in $v_i = (a_1,\ldots,a_d)$ where a_j is the observation of the j^{th} attribute do

- $a_j' \leftarrow Transform\ (a_l, op_l, noise_j)$

End

3.3 SLICING WITH CLUSTERING TECHNIQUES

Cluster analysis is the technique of grouping the related records collectively that is used for further processing and classification [16]. The Slicing based anonymization method partition the data set into vertical partition and horizontal column. In vertical partitioning section correlated attributes are grouped into one column and the column does not have any correlation among other column. In tuple partitioning segment, tuples are grouped into the bucket and each column attributes break the correlation between the attributes. For enhancing the slicing algorithm, it has to be blended with the clustering techniques [15].

In the vertical partitioning phase associated attributes are mixed collectively in one column. This preserves privacy and utility. In the beginning, the data points are distributed in the data space. The grouping algorithm is functional for combination pertinent SA and for this reason reduces dimensionality. A new Advanced Clustering Algorithm (ACA) [4] for segregating the characteristics into supports is added that can successfully support in augmenting the grouping pace and hence limit the complexity concerned in computation. It keeps two data structures, former for containing the characteristics of groups and the latter for containing the lowest distance among the attributes. In this type of manner it could be exploited as a part of the subsequent cycle. Pearson correlation coefficient offers a degree of the correlation among the input terms. The correlation amongst the attributes is intended by,

$$\rho(\mathrm{X},\mathrm{Y}) = \frac{\sum_{i=1}^{n}(x_i-\overline{x})(y_i-\overline{y})}{\sqrt{\sum_{i=1}^{n}(x_i-\overline{x})^2}\sqrt{\sum_{i=1}^{n}(y_i-\overline{y})^2}} \tag{7}$$

$$\overline{x} = \frac{1}{n}\sum_{i}^{n} x_i \tag{8}$$

$$\overline{y} = \frac{1}{n}\sum_{i}^{n} y_i \tag{9}$$

The value varies between -1 to 1. The distance amongst two attributes is specified by

$$d_P = \frac{1-\rho(\mathrm{X},\mathrm{Y})}{2} \tag{10}$$

If the distance is least or equal, then the characteristic will keep on in its cluster which was allocated to it in the previous sequence. By this method, there is no motivation to calculate the distance from this characteristic group to the subsequent k-1 groups, thus reducing the dispensation time till the k-1 cluster emphases. Besides, the separation from the current group to all k groups is to be calculated and the neighboring group has to be positioned. This can increase the speed of grouping competently and minimize the computational difficulty. This procedure goes till the stop condition is accomplished.

Procedure:

Begin

1. Describe one subgroup of attributes from the given dataset.
2. Repeat step 3 for $m = 1$ to N.
3. For each sub group middle attribute be the centroid
4. For each attribute calculate the nearest centroids and assign to next cluster
5. Choose smallest of smallest distance from the cluster's center
6. Repeat the process for the dataset for all clusters
7. Combine the two nearest clusters
8. Recalculate the cluster center for the collective group till the elements of cluster are dissimilar

End

Horizontal Segmentation is done by using Metaheuristic Fireflies Algorithm with Minkowsi Distance Measure (MFAMD) which forms the buckets from the collection of tuples. So this procedure is called as the Tuple Segmentation. The following steps define the proposed algorithm.

1. $Q = \{T\}$;
2. SB = Null.
3. If Q contains the tuple T, then remove the Bucket B from Q
4. Split the Bucket into two different Bucket using Fireflies algorithm
   - First check the tuples from the Q
   - Set the Objective function for that Q
   - Then Calculate the Intensity by using that objective function (Max or Min)
     i. Calculate attractiveness by Minkowsi based tuples distance
   - Using the Intensity and Attractiveness value form the bucket from Q.
5. Then check the diversity of the tuples.

From the above algorithm, the tuples are segment into different bucket and those neighbor tuples are analyzed for further bucket formation processing. The work is based on the flashing behavior of firefly which has two important parameters: Intensity and attractiveness. It uses these features to identify similar tuples in a bucket. The intensity value is used to identify a sensitive tuple via an objective function. The attractiveness is calculated by fireflies' distance between the other fireflies by applying Minkowsi Distance measure. Based on the attractiveness the tuples are grouped into buckets while assuring l diversity in each bucket.

4. EXPERIMENTAL ANALYSIS

The research was executed in Java and approved out on a 3.3 GHz Intel Core processor with 20 GB hard disk and 3 GB RAM having Windows XP operating System.The recital of the procedure is confirmed in excess of the adult datasets attained from the OCC 7 which includes 7 attributes and the second dataset is the OCC-15 dataset, which includes all 15 attributes. In the first experiment, the performance metrics measured the classification accuracy of the anonymised data with the existing system. In the next experiment, privacy-utility tradeoff between the system proposed and the existing approaches is measured.

4.1 PERFORMANCE METRICS

The performance metrics measured the clustering accuracy of the anonymised data using the parameters: True Positive (*TP*), True Negative (*TN*), False Positive (*FP*), False Negative (*FN*), and Detection Accuracy (*DA*).

4.1.1 True positive (TP):

True Positive (TP) is the ratio of positive cases that were correctly identified, as intended by means of the equation:

$$TP = (\textit{Number of correctly clustered data}) / (\textit{Total datasets}) \times 100$$

4.1.2 True Negative (TN):

True Negative (TN) is sketched as the ratio of negatives cases that were classified correctly, as deliberate with the equation:

$$TN = (\textit{Number of incorrectly clustered data}) / (\textit{Total datasets}) \times 100$$

4.1.3 False Positive (FP):

False Positive (FP) is the ratio of negatives cases that were incorrectly classified as positive, as intended by means of the equation:

$$FP = (\textit{Number of correctly clustered data}) / (\textit{Total datasets}) \times 100$$

4.1.4 False Negative (FN):

False Negative (FN) is the ratio of positives cases that were incorrectly classified as negative, as intended by means of the equation:

$$FN = (\textit{Number of incorrectly clustered data}) / (\textit{Total datasets}) \times 100$$

4.1.5 Classification Accuracy (DA):

Accuracy is a global rationon condition that the proportion of total well-classified images.

$$DA = (TP + FP) / (TP + FN + TN + FP) \times 100 \quad (11)$$

The detection precision is consideredby means of the sum of true positive and true negative alienated by the sum of true positive, false negative, true negative and false positive.

Table.2. Performance Analysis

Technique & Data Set		TP	TN	FP	FN	ACC
K- Means	OCC – 7	82	18	72	28	77.0
	OCC -15	89	11	88	12	88.0
Fuzzy C Means	OCC – 7	75	25	73	27	74
	OCC -15	83	17	77	23	80
Translation	OCC – 7	76	24	89	11	82.5
	OCC -15	85	15	91	09	87.6
Scaling	OCC – 7	69	31	64	36	66.5
	OCC -15	86	14	76	24	81.34
Rotation	OCC – 7	91	09	89	11	90.45
	OCC -15	96	4	88	12	95.36
Slicing with HDT	OCC – 7	93	07	91	9	92.98
	OCC -15	98	2	89	11	96.92

From the above table, it is evident that our proposed algorithm works well, when associated to other algorithms. Next to our algorithm, Rotation transformation approach proves better accuracy rate of 90.45% and 95.36% respectively.

4.2 PRIVACY / UTILITY

The proposed methodology analyzes the privacy-utility tradeoff between the system proposed and the existing fuzzy, translation, scaling and rotation approaches.

Privacy loss is adversary understands about the sensitive values of particular individuals from the anonymized data whereas utility loss is measured by the information loss about the sensitive values from the original data. We obtain a set of (P_{loss}, U_{loss}) pairs, one for each anonymized dataset. We design the (P_{loss}, U_{loss}) pairs on a 2-dimensional space, where the *x*-axis represents the privacy loss, P_{loss} and the *y*-axis represent the utility loss, U_{loss}.

The privacy loss for a tuple *t* is measured as the distance between *S* and *P*(*s*) where, *S* is the distribution of the sensitive attribute in the original table and P(s) is the distribution of the sensitive attribute in the anonymised table. We use the JS-divergence distance measure:

$$P_{loss}(t) = JS(S, P(s)) = [KL(S, M) + KL(P(s), M)] \quad (12)$$

where, $M = 0.5(S + P(s))$ *KL*-divergence:

$$KL(S,P) = \sum_i \frac{q_i \log q_i}{p_i} \quad (13)$$

The utility of the anonymised data set is measured using aggregate query answering with the "COUNT" operator:

SELECT COUNT (*) FROM Table.

WHERE $v_{i1} \in V_{i1}$ AND ... $v_{idim} \in V_{idim}$ AND $s \in Vs$

where, v_{ij} are the quasi-identifier value for attribute and *s* is the sensitive attribute value. For each query, run the query on the original table and the anonymized table. Then denote the actual count from the original table as act_{countq}. Similarly denote the reconstructed count from the anonymized table as re_{countq}.

Then the Average Relative Error (ARE) is computed over all queries as:

$$\rho = \frac{1}{|Q|} \sum_{q \in Q} \frac{\left| rec_{count_q} - act_{count_q} \right|}{act_{conf_q}} \times 100 \quad (14)$$

where, *Q* is the set of queries generated. Smaller errors indicate higher utility of the data. We randomly generate 1000 aggregate queries of the above form i.e., $|Q| = 1000$.

When comparing the privacy and utility values of the existing method with the hybrid method, it clearly indicates that the proposed hybrid method provides better privacy and utility for the adult datasets. Among the three hybrid methods rotation function gives the lower utility.

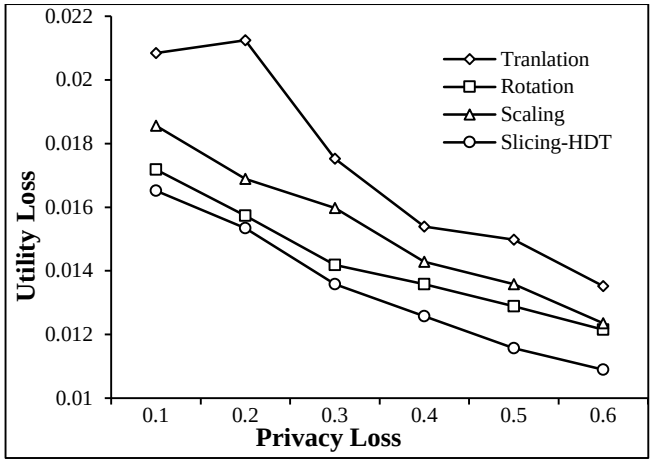

Fig.2. Privacy-Utility Tradeoff: U_{loss} vs. P_{loss}

5. CONCLUSION

The important goal of this work is to preserve the SA attributes with three layered protection using HDT. The masked data are anonymised in addition using slicing algorithm to preserve confidentiality over horizontal and vertical segregating. We have analyzed different data transformation methods like fuzzy C means, translation, rotation and scaling upon two different datasets. On analysis, we found that our multiple objective optimization algorithms outperform the others and produced better result in terms of accuracy, utility and privacy.

ACKNOWLEDGEMENT

The work has been supported by the University Grants Commission (UGC)-New Delhi, India and the grant number is MRP-5711/15 (SERO /UGC) January 2015.

REFERENCES

[1] Vassilios S. Verykios, Elisa Bertino, Igor Nai Fovino, Loredana Parasiliti Provenza, Yucel Saygin and Yannis Theodoridis, "State-Of-The-Art in Privacy Preserving Data Mining", *ACM Sigmod Record*, Vol. 3, No. 1, pp. 50-57, 2004.

[2] Murat Kantarcioglu, Jiashun Jin and Chris Clifton, "When Do Data Mining Results Violate Privacy?", *Proceedings of the 10th ACM International Conference on Knowledge Discovery and Data Mining*, ACM, pp. 599-604, 2004.

[3] Rakesh Agrawal and Ramakrishnan Srikant, "Privacy Preserving Data Mining", *Proceedings of the ACM International Conference on Management of Data*, pp. 439-450, 2000.

[4] Amanpreet Kaur Toor and Amarpreet Singh, "An Advanced Clustering Algorithm (ACA) for Clustering Large Data Set to Achieve High Dimensionality", *Computer Science Systems Biology*, Vol. 7, No. 4, pp. 115-118, 2014.

[5] Arik Friedman, Ran Wolff and Assaf Schuster, "Providing k-Anonymity in Data Mining", *The Vldb Journal*, Vol. 17, No. 4, pp. 789-804, 2008.

[6] Latanya Sweeney, "k-Anonymity: A Model for Projecting Privacy", *International Journal on Uncertainty fuzziness*

and Knowledge-Based Systems, Vol. 10, No. 5, pp. 557-570, 2002.

[7] Adam Meyerson and Ryan Williams, "On the Complexity of Optimal k-Anonymity", *Proceedings of 23rd ACM SIGMOD-SIGCAT-SIGART Symposium on Principles of Database Systems*, pp. 223-228, 2004.

[8] Pierangela Samarati, "Protecting Respondents' Identities in Microdata Release", *IEEE Transactions on Knowledge and Data Engineering*, Vol. 13, No. 6, pp. 1010-1027, 2001.

[9] Tiancheng Li and Ninghui Li, "Optimal k-Anonymity with Flexible Generalization Schemes through Bottom-Up Searching", *Proceedings of 6th IEEE International Conference on Data Mining-Workshops*, pp. 518-523, 2006.

[10] Vijay S. Iyengar, "Transforming Data to Satisfy Privacy Constraints", *Proceedings of 8th ACM International Conference on Knowledge Discovery and Data Mining*, pp. 279-288, 2002.

[11] Ke Wang, P.S. Yu and S. Chakraborty, "Bottom-Up Generalization: A Data Mining Solution to Privacy Protection", *Proceedings of 4th IEEE International Conference on Data Mining*, pp. 249-256, 2004.

[12] Benjamin C.M. Fung, Ke Wang and Philip S. Yu, "Anonymizing Classification Data for Privacy Preservation", *IEEE Transactions on Knowledge and Data Engineering*, Vol. 19, No. 5, pp. 711-725, 2007.

[13] M. Ercan Nergiz and Chris Clifton, "Thoughts on k-Anonymization", *Data and Knowledge Engineering*, Vol. 63, No. 3, pp. 622-645, 2007.

[14] B. Karthikeyan, G. Manikandan and V. Vaithiyanathan, "A Fuzzy based Approach for Privacy Preserving Clustering", *Journal of Theoretical and Applied Information Technology*, Vol. 32, No. 2, pp.118-122, 2011.

[15] Sridhar Mandapati, Raveendra Babu Bhogapathi and Ratna Babu Chekka, "A Hybrid Algorithm for Privacy Preserving in Data Mining", *International Journal of Intelligent Systems and Applications*, Vol. 5, No. 8, pp. 47-53, 2013.

[16] Alex A. Freitas, "*Evolutionary Algorithms for Data Mining*", The Data Mining and Knowledge Discovery Handbook, pp. 435-467, 2005.

[17] Matthew S. Gibbs, Graeme C. Dandy and Holger R. Maier, "A Genetic Algorithm Calibration Method based on Convergence Due to Genetic Drift", *Information Sciences*, Vol. 178, No. 14, pp. 2857-2869, 2008.

[18] Jinhua Zhang, Jian Zhuang, Haifeng Du and Sunan Wang, "Self-Organizing Genetic Algorithm based Tuning of PID Controllers", *Information Sciences*, Vol. 179, No. 7, pp. 1007-1018, 2009.

[19] Lior Rokach, "Genetic Algorithm-based Feature Set Partitioning for Classification Problems", *Pattern Recognition*, Vol. 41, No. 5, pp. 1693-1717, 2008.

[20] Melanie Mitchell, "*An Introduction to Genetic Algorithms*", 1st Edition, MIT Press, 1996.