



Prevention of Direct and Indirect Discriminants Method and Evaluation Parameter

Rajni Mishra, Sandeep Kumar, Prof. Aishwarya Mishra

Department of Computer Science and Engineering

IES College of Technology

Bhopal India

Abstract—Extraction of the important information from large set of data is done in data mining. But this information is sometime tends to extract information which harm the personal identity. So privacy preserving mining is new era of research. Keeping this motive paper work to provide the privacy for the discriminate prevention from the large dataset. Here by using Aprior algorithm association rules are generate and preserve the dicriminant items from the dataset by decreasing the support value of the discriminate item. Here by decreasing the the dicriminant item will prevent different rule generation. Results shows that proposed approach is better on the different evaluation parameter include the time and originality.

Index Terms— Data mining, Data Perturbation, Multiparty Privacy Preserving.

I. INTRODUCTION

The aim of data mining [1, 10, and 11] is to extract useful information, such as patterns and trends, from large amounts of data. In their fight against crime and terrorism, many governments are gathering large amounts of data to gain insight into methods and activities of suspects and potential suspects. This can be very useful, but usually at least part of the data on which data mining is applied is confidential and privacy sensitive. Examples are medical data, financial data, etc. This raises the question how privacy, particularly of those who are innocent, can be ensured when applying data mining. Furthermore, the results of data mining can lead to selection, stigmatisation and confrontation [7]. False positives and false negatives are often unavoidable, resulting in the fact that people are frequently being judged on the basis of characteristics that are correct for them as group members, but not as individuals as such [18]. In the context of public security, false positives may result in investigating innocent people and false negatives may imply criminals remain out of scope.

Main purpose of data mining is to retrieve important information from the dataset inform of patterns of items, it is like an trend that thing get repeat regularly in the dataset. In order to find the pattern which indicate the normal activity of the terrorist, crimals, customers, viruses, etc[7, 11].. This mining is very useful. This kind of information gathering from the raw data is harmul in many areas as well because it lead to the kind of separation from the uncommon part tend to generate the information which may give information in other sense as well. Suppose an intruder need to gather personal information from the dataset like medical, financial, social etc. This lead to new area of how to protect the personal information of the people from the data miners. So in order to release such kind of data which are fruitful for those people who want to get illegal information then it need to make some modification in the dataset. So in order to provide security for the public false negative may imply criminals out of scope.

A priori protection may be realised by protecting input data and access to input data. However, removing key attributes such as name, address and social security number of the data subject is insufficient to guarantee privacy; it is often still possible to uniquely identify particular persons or entities from the data, for instance by combining different attributes. Since the results of data mining are often used for selection, a posteriori protection is also desirable, in order to ensure that the output of data mining is only used within the imposed ethical and legal frameworks. This implies, for instance, that data mining results on terrorism, where data was collected within extensive jurisdiction of secret services, cannot be used just like that for shoplifting or car theft, where data was collected within limited jurisdiction of the police.

II. RELATED WORK

Many researchers have given details, algorithms and experimental results on pre-processing methods are presented in [4,5]. The aim of all these methods is to transform the original data so that it will make minimum impact on the data and on legitimate decision rules, and the main purpose the work will be fulfill of making unfair decision rule that can be

mined from the transformed data. The measure of the algorithm are depend on the, the metrics that specify which records should be changed, how many records should be changed and how those records should be changed during data transformation are developed so that it will make minimum impact on the original data. Few works are done base on the assumptions such as the class attribute in the original dataset is binary other is the database of discriminatory and redlining rules as output of a discrimination measurement phase based on measures proposed in [1,2].

In case of Pre-processing there are methods that can identify those rules or attributes in the database that is obtained from the source data then remove, modify those discriminatory rules or attributes biases contained in the original data so that no unfair decision rule can be mined from the transformed dataset by using any of the data mining algorithms. The pre-processing approaches of data transformation and hierarchy-based generalization can be adapted from the privacy preservation literature [5,11].

In case of the In-processing there are many approaches that change the data mining algorithms in such a way that the obtaining models is free from unfair decision rules [10]. For example, an alternative approach to cleaning the discrimination from the original dataset is proposed in [10] whereby the non-discriminatory constraint is embedded into a decision tree learner by changing its splitting criterion and pruning strategy through a novel leaf re-labeling approach. Although it is found that in-processing discrimination prevention algorithms are depends on the special purpose data mining approaches as standard data mining algorithms cannot be used because they ought to be adapted to satisfy the non-discrimination requirement.

III. BACKGROUND

Basic Notions

The data set is a combination of object of data and their attribute .Let we see original dataset to data set

An item is an attribute along with its value, e.g. {Race=black}. An item set, i.e. X, is a collection of one or more items, e.g. {Foreign worker=Yes, City=NYC}. A classification law is an expression $X \rightarrow C$, where C is a class item (a yes/no decision), and X is an item set containing no class item, e.g. {Foreign worker=Yes, City=NYC} \rightarrow {hire=no}. X is said the premise of the law.

Support(s) of an association law is defined like the percentage/fraction of data that contain X U Y to the total number of data in the database. that contain X U Y to the total number of records.

$$\text{Support}(X \rightarrow Y) = (XUY) / D$$

Confidence: Confidence of an association rule is defined as the percentage/fraction of the number of transactions contain X U Y to the total number of records that contain X, where if the percentage exceeds the threshold of confidence an interesting association rule $X \rightarrow Y$ can be generated.

$$\text{Confidence}(X \rightarrow Y) = (XUY) / X$$

The association rules measure of strength by confidence suppose the association laws of confidence ($X \rightarrow Y$) is 80% that means that 80% of that transaction and x and y also contain together .by users minimum confidence is already defined with specific laws.

Elift: Pedreschi et al. [12] generate the new method of evaluation of rules from the measure that is elift which is the ratio of the confidence of the rule to the confidence of the non discriminatory items in that rule.

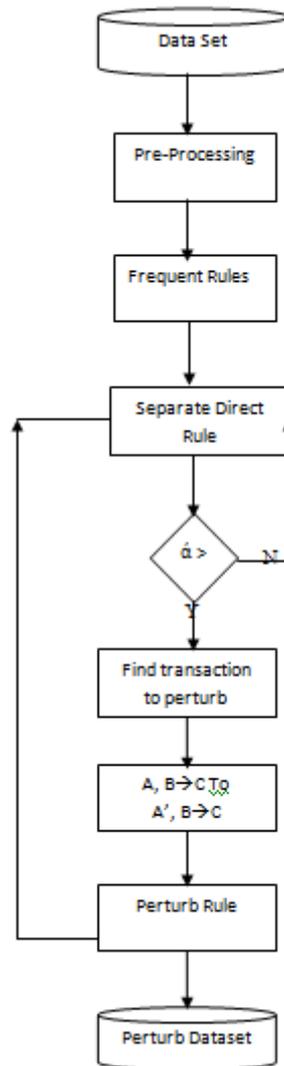
$$\text{Elfit} = \text{Conf}(AUB \rightarrow C) / \text{Conf}(B \rightarrow C)$$

IV. PROPOSED WORK

Pre-Processing: As the dataset is obtain from the above steps contain many unnecessary information which one need to be removed for making proper operation. Here data need to be read as per the algorithm such as the arrangement of the data in form of matrix is required.

Generate Rules: In order to hide the information from the dataset one approach is to reduce the support and confidence of the desired item. For finding the item set which is most desired one has to find that the frequent pattern in the dataset. There are many approaches of pattern finding in the dataset which are are most frequent one of the most popular is aprior algorithm is use in this work.

Separate Direct and Indirect Rules: Now from the generate rule step one can get bunch of rules then it is required to separate those rules from the collection into direct and indirect rule set. Those rules which contain dicriminant items are identified as the direct rules which those not contain are indirect rules. This can be understand as the Let A, B \rightarrow C where A is set of discriminant item then this rule is direct rule, where B, C are non discriminant items. If D, B \rightarrow C is a rule and D is the non discriminate item set the this rule is not direct rule.



Now all direct rules are need to find that either it is α discriminate rule or not for this first find the elift value of the rule then then those rules whose elift value are more then the α value is term as the α discriminatory rule.

Perturb Transaction: Now next step is to calculate number of transaction that need to be modified in order to hide the rules. For this follow steps

1. Now Find support that is lacking from the maximum support
Noise = (Max_support – Rule_support)
2. Find fake transaction number for each rule by
Transaction = (Noise x Dataset_size)/100

Perturbation:

In order to hide that rule many approaches has been done that is mention in the table below

	Original Rule	Perturb Rule
Previous	A, B → C	A, B → C'
Proposed	A, B → C	A', B → C

By change in the discriminate item directly from A to A' where A' is the opposite of A. Another advantage of this is it is not required to suppress the indirect rule seperatly as the indirect rule which is obtain from the combination of the discriminating items. So by suppressing the discriminating item only all kind of rule get hide.

Proposed Algorithm:

Input: DS (Original Dataset), α

Output: PDS (Perturb Dataset)

1. DS ← Pre-Process(DS)
2. PDS = DS

3. $FR[n] \leftarrow \text{Aprior}(DS) // n \text{ number Association rule}$
4. Loop 1:n
5. If $FR[n] \cap DI$
6. $DR \leftarrow FR[n]$
7. Endif
8. End Loop
9. Loop 1:n
10. $E \leftarrow \text{Elift}(DR[n])$
11. If $E > \alpha$
12. Transaction = Perturb_Transaction(DR[n])
13. Loop 1:m
14. $PDS \leftarrow \text{Perturbation}(DS[m])$
15. EndLoop
16. EndIf
17. End Loop

V. EXPERIMENT AND RESULT

This section presents the experimental evaluation of the proposed perturbation and de-perturbation technique for privacy prevention. To obtain AR this work used the Apriori algorithm [1], which is a common algorithm to extract frequent rules. All algorithms and utility measures were implemented using the MATLAB tool. The tests were performed on an 2.27 GHz Intel Core i3 machine, equipped with 4 GB of RAM, and running under Windows 7 Professional.

Dataset:

In [9] it has use Adult dataset where it contain different discriminating item set such as country, Gender, Race, 1996. This data set consists of 48,842 records, split into a “train” part with 32,561 records and a “test” part with 16,281 records. The data set has 14 attributes (without class attribute). For our experiments with the Adult data set, we set $DI = \{\text{Gender}=\text{Female}\}$ and salary greater then the 50k\$.

Evaluation Parameters

There are two approaches to evaluate the discriminating algorithm developed which can specify the quality of the work first is Discrimination Removal while second is data quality after the implementation of the algorithm. Normally balancing both is quit difficult as if data quality need to maintain then some of the rules will be unaffected and over all purpose will be not be solve while in case of maintaining discriminating rule less data [11], dataset the quality will definite degrade as it need to either change or remove from the dataset.

Direct Discrimination Prevention Degree (DDPD). This measure quantifies the percentage of discriminatory rules that are no longer discriminatory in the transformed dataset.

Direct Discrimination Protection Preservation (DDPP). This measure quantifies the percentage of the protective rules in the original dataset that remain protective in the transformed dataset.

Measuring Data Quality

The second aspect to evaluate discrimination prevention methods is how much information loss (i.e. data quality loss) they cause. To measure data quality, two metrics are proposed in Verykios and Gkoulalas-Divanis (2008):

Execution time : Third parameter is to evaluate execution time time of the algorithm that is time taken by the proposed method for execution. Algorithm time is expect after the evaluation of the direct and indirect rules.

Results: In order to evaluate this work different α value are use accordingly the perturbation of the dataset is obtained.

Table 2 Represent results of originality in dataset at different α values.

α vlues	Originality	
	Proposed Work	DRP+IRP[11]
1	99.9669	99.9581
1.1	99.9746	99.9726
1.2	99.9803	99.9785

From above table it is obtained that with the increase of the α values the perturbation get decrease while with the decrease of the α values perturbation value get increase. One more important factor is that proposed work maintain the originality more as compare to the previous one in [11] in all the α values.

Table 3 Represent results of DDPD and DDPP values at different α values.

α	Proposed Work		DRP+IRP[11]	
	DDPD	DDPP	DDPD	DDPP
1	100	0	100	0
1.1	100	0	100	0
1.2	100	0	100	0

From above table 3 it is obtained that that proposed work maintain the same DDPD and DDPP values as in the previous one in [11] in all the α values. As all the rules which are α discriminatory are hide by the [11] and proposed work so the values obtain is 100.

Table. 4 Represent results of execution time of both method at different α values.

α vlues	Execution Time	
	Proposed Work	DRP+IRP[11]
1	3.5063	66.6521
1.1	3.6535	66.3257
1.2	3.5767	65.8821

From above table 4 it is obtained that with the increase of the α values the execution time get increase, while with the decrease of the α values perturbation value get decrease. One more important factor is that proposed work maintain the low execution time as compare to the previous one in [11] in all the α values.

VI. CONCLUSION

Researchers are working in different field out of which Preserving privacy minning is one of the new and important era. This paper focus on two thing first is of provide preserving for discriminant items in the dataset next is to maintain the originality of the data. Here by changing the hidden rule from the discimnant to non discriminant one privacy is maintain. Results shows that performace of the proposed work is better in all section of evaluation parameter such as originality and execution time. In future, more work need for the same field for cloud storage and distributed databases.

REFERENCES

- [1] Pedreschi, D., Ruggieri, S. & Turini, F. (2008). Discrimination-aware data mining. Proc. of the 14th ACM International Conference on Knowledge Discovery and Data Mining (KDD 2008), pp. 560-568. ACM.
- [2] Pedreschi, D., Ruggieri, S. & Turini, F. (2009a). Measuring discrimination in socially-sensitive decision records. Proc. of the 9th SIAM Data Mining Conference (SDM 2009), pp. 581-592. SIAM
- [3] Ruggieri, S., Pedreschi, D. & Turini, F. (2010). Data mining for discrimination discovery. ACM Transactions on Knowledge Discovery from Data, 4(2) Article 9.
- [4] Hajian, S., Domingo-Ferrer, J. & Martinez-Ballesté, A. (2011a). Discrimination prevention in data mining for intrusion and crime detection. Proc. of the IEEE Symposium on Computational Intelligence in Cyber Security (CICS 2011), pp. 47-54. IEEE.
- [5] Hajian, S. & Domingo-Ferrer, J. (2012). A methodology for direct and indirect discrimination prevention in data mining. Manuscript.
- [6] Yin, X. & Han, J. (2003). CPAR: Classification based on Predictive Association Rules. In Proc. of SIAM ICDM 2003. SIAM.
- [7] Verykios, V. & Gkoulalas-Divanis, A. (2008). A survey of association rule hiding methods for privacy. In C. C. Aggarwal and P. S. Yu (Eds.), Privacy- Preserving Data Mining: Models and Algorithms. Springer.
- [8] [15] Meij, J. (2002) *Dealing with the data flood; mining data, text and multimedia*, The Hague: STT Netherlands Study Centre for Technology Trends.
- [9] Pedreschi, D., Ruggieri, R., and Turini, F. (2008) *Discrimination-aware Data Mining*. In Proceedings of the 14th ACM SIGKDD Conference on Knowledge Discovery and Data Mining.
- [10] Calders, T., & Verwer, S. (2010). Three naive Bayes approaches for discrimination-free classification. Data Mining and Knowledge Discovery, 21(2):277-292.
- [11] Sara Hajian and Josep Domingo-Ferrer "A Methodology for Direct and Indirect Discrimination Prevention in Data Mining" IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING, VOL. 25, NO. 7, JULY 2013