Volume 5, Issue 4, 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Data mining for Discrimination Prevention

Supriya M. Manglekar, V. K. Bhusari
Department of Computer Engineering, Pune University,
Maharashtra, India

Abstract— Data mining is important technology for extracting useful data hidden in large collections of data. Discrimination refers unfair or unequal treatment of people based on membership to a particular category or a minority. Automated data collection and data mining techniques such as classification rule mining have paved way to making automated decisions, like loan granting/denial, insurance premium computation etc. If training data sets are biased regards discriminatory attributes like gender, race etc. discrimination decisions may ensue. For this reason, antidiscrimination techniques including discrimination discovery and prevention have been introduced in data mining. Discrimination can be either direct or indirect. In this paper, we tackle discrimination prevention in data mining and propose new techniques applicable for direct or indirect discrimination prevention individually or both at same time. Experimental evaluation demonstrate that proposed techniques are effective at removing direct and/or indirect discrimination biases in the original data set while preserving its data quality

Keywords: discrimination, antidiscrimination, discrimination prevention,

I. INTRODUCTION

In sociology, discrimination is viewed as act of unfairly treating people on the basis of their belonging to a specific group. For example, individuals may be discriminated because of their gender, race etc [2]. Services in the information society allow for automatic and routine collection of large amount of data. Those data are often used to train association/classification rules in view of making automated decisions, like loan granting/denial, insurance premium computation etc There is list of antidiscrimination acts, which are laws designed to prevent discrimination on the basis of a number of attributes(e.g., race, disability , religion, age). For example, the European Union implements the principle of equal treatment between men and women in the access to and supply of goods and services or in matters of employment and occupation.[1]

Discrimination can be either direct or indirect. Direct discrimination consist of rules or procedures that explicitly mention minority or disadvantaged groups based on sensitive discriminatory attributes related to group membership. For example, Foreign worker=YES. Indirect Discrimination consist of rules or procedures that while not explicitly mention discriminatory attributes, intentionally or unintentionally could generate discriminatory decisions. For example, zip=10451 indicating that a certain zip code correspond to a deteriorating area. Indirect discrimination could happen because of the availability of some background knowledge

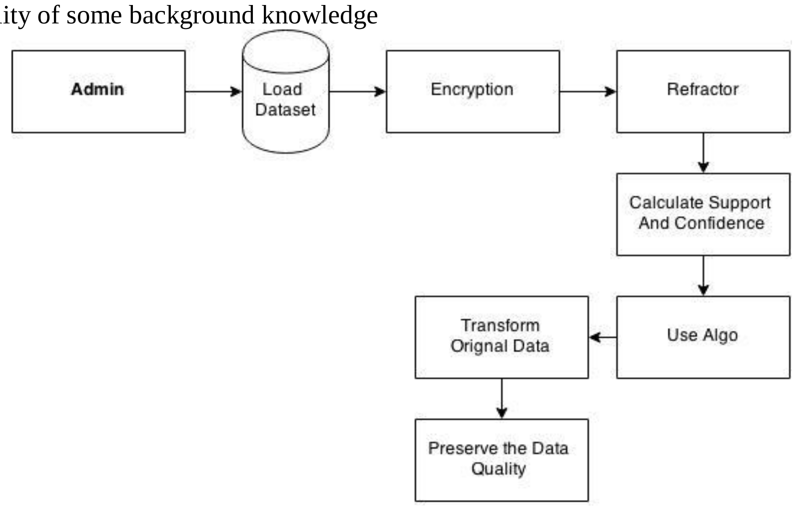


Fig. 1 System Architecture

A. Discrimination Discovery

It is based on formalizing legal definitions of discrimination and proposing quantative measures for it. These measures were proposed [3].This approach has been extended to encompasses to encompass statistical significance of extracted pattern of discrimination[4] and it has been implemented as reported in [5].Data mining is powerful aid for discrimination analysis, capable of discovering the patterns of discrimination that emerges from the data.

B. Discrimination Prevention

It consist of inducing patterns that do not lead to discriminatory decisions even if trained from a dataset containing them. Clearly a straightforward way to handle discrimination prevention would consist of removing discriminatory attributes from the dataset. However, there may be other attributes that are highly correlated with the sensitive one. Hence one might decide to remove also those highly correlated attributes as well. Although this would solve discrimination problem, in this process much useful information would be lost. Hence another challenge regarding discrimination prevention is to find optimal trade-off between anti-discrimination and usefulness of training data

II. LITERATURE SURVEY

1. Classification With No Discrimination By Preferential Sampling

We can remove the sensitive data instead of relabeling it. The new solution to the CND problem by introducing a sampling scheme for making the discrimination free instead of relabeling the data set. The algorithm is used in this paper is classification algorithm. The goal of classification is to accurately predict the target class for each care in the data. Predicts categorical labels and classify the data based on the training set and the values in a classifying attribute and uses it in classifying new data. The techniques used in this paper is Pre-processing, Preferential sampling, Over sampling, Uniform sampling. In preprocessing there are a lot tangential and excess data present or noisy and so knowledge uncovering during the aiming stage are a lot of elaborated . Data preparation and filtering steps can considerable amount of processing period. Data,pre-processing includes cleaning, normalization,transformation and characteristic extraction selection.In this paper disadvantage is Discrimination were removed in ethical and legal region.

2. Fast Algorithm For Mining Association Rules

Fast algorithm is an efficient algorithm used to avoid the discrimination in data mining. In this paper algorithm apriori, aprioritid, AIS algorithm, apriorihybrid algorithm. The apriori algorithmic rule are the adult detail sets by the early authorize comprised reached aim the fresh candidate detail . Pruning comprised represented applying the information that some subdivision of itemset.

The difference for determining the support the database is not used after the first pass. In the AIS algorithm .In the AIS algorithm involves two concepts are extension of an item set, determining what should be in the candidate item set .The apriori hybrid algorithm is Uses apriori in the early passes and later shifts to aprioritid .In this paper disadvantages is An extra cost is sustained when shifting from apriori to aprioritid.

3. Discrimination Prevention In Data Mining Since Intrusion And Crime Detection

In this paper techniques is used the anti discrimination techniques. Antidiscrimination law to the natural law about the correct by people to comprise addressed. In the governmental involvement people essential comprise addressed on active equal base in some cause by sex activity, age, race, nationality. The approaches are used pre processing, post processing. The pre processing is data pre processing is the important process in the data mining. In there are more than tangential and excess information represent or noisy and uncertain information, and then knowledge discovery on the aiming point are heavier

The analyzed information that are not represented carefully screened out as much troubles may develop misleading answers. The post processing are the action by categorization through with large amounts of information and cleaning our applicable data. Data mining in acknowledgment to initiative resource preparation are the statistical and ordered analysis from large sets by transaction information mining in relation to enterprise resource planning is the statistical and logical analysis of large sets of transaction data. the algorithm used in this paper is not efficient this is main drawback of this paper.

III. IMPLEMENTATION

A. Basic Definations

An item is an attribute along with its value, e.g.{Gender=Female}

Classification rule is an expression X → C ,where C is class item(yes/no decision) and X is an item-set containing no class item e.g. {Foreign worker=Yes, City=NYC}→{hire=no}

The Support of an itemset, supp(X), is the fraction of records that contain the itemset X. We say that a rule X ! C is completely supported by a record if both X and C appear in the record.

$$conf(X \rightarrow C) = \frac{supp(X,C)}{supp(X)} \quad (1)$$

The confidence of a classification rule, conf(X → C), measures how often the class item C appears in records that contain X. Hence if supp(X) > 0

B. Discrimination Measures

The Pedreschi et al.[3], translated the qualitative statements in existing laws, regulations and legal cases into qualitative formal counter parts over classification rules and they introduced a family of the degree of discrimination of PD rule.In our contribution we use extended lift(elift)measure. Let A,B → C be a classification rule with conf(B→C)>0.

The extended lift of the rule is The idea here is to evaluate the discrimination of a rule by the gain of confidence due to presence of the discriminatory items(i.e.A) in the premise of the rule. elift is defined as the ratio of confidence of two rules: with and without the discrimination items. Whether the rule is to be considered discriminatory van be assessed by thresholding elift as follows Let α be a fixed threshold. A
PD classification rule c=A,B → C is -protective w.r.t. elift if elift(c) < α . Otherwise, c is discriminatory. Consider rule c=Race=Black,Zip=43700!Hire =YES
If =1.4 and elift=1.46, rule c is 1.4-discriminatory. D. Mathematical Model
DB: Original Database
FR: Frequent classification rule
MR: Database of -discriminatory rules extracted from database DB
: fixed threshold
DI: Set of predetermined discriminatory items in DB
1 Input: DB,FR,MR, ά ,DI
2 Output: DB'(Transform Data set)
3 for each r': A,B→C ϵ MR do
4 FR ← FR – {r'}
5 DB ←All records completely supporting – A,B→C
6 for each dbϵDB do
7 compute impact(db_c) = I{ r_a ϵ FR}Idb_c supports the premise of r_a
8 end for
9 Sort DB_C
10: while conf($r^{'}$) ≥ ά.conf(B->C) do
11: Select first record in DB_C
12: Modify discriminatory item set of DB_C from :A to A in DB
13: Recompute conf($r^{'}$)
14: end while
15: end for
16: Output: DB'= DB

C. Measuring Discrimination Removal

Discrimination prevention methods should be evaluated based on two aspects: discrimination removal and data quality. How successful the method is at removing all evidence of direct and/or indirect discrimination from the original dataset. To measure discrimination removal, four metrics are proposed
(1) Direct Discrimination Prevention Degree (DDPD):
This measure quantifies the percentage of discriminatory rules that are no longer discriminatory in the transformed dataset.
(2) 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.
(3) Indirect Discrimination Prevention Degree (IDPD):
This measure quantifies the percentage of redlining rules that are no longer redlining in the transformed dataset.
(4) Indirect Discrimination Protection Preservation (IDPP): This measure quantifies the percentage of non-redlining rules in the original dataset that remain non-redlining in the transformed dataset.
Since the above measures are used to evaluate the success of the proposed methods in direct and indirect discrimination prevention.

D. Privacy Preserving Data mining

Privacy Preserving Data mining has become more important in recent years because of the increasing ability to store personal data about users and increasing sophistication data mining algorithms to leverage this information. This has lead to concerns that the personal data may be misused for variety of purposes. In order to alleviate these concerns we have been proposed techniques such as cryptography and information hiding in order to perform the data mining tasks in privacy-preserving way.

The Advanced Encryption Standard (AES) was published by NIST (National Institute of Standards and Technology) in 2001. AES is a symmetric block cipher that is intended to replace DES as the approved standard for a wide range of applications. At that time, triple-DES had become popular, but it was too slow and the 64-bit block length was too small. The double-DES is not much harder to break by brute-force than DES using a "meet-in-the-middle" attack
Requirements:
The requirements for the algorithms were as follows:

- The algorithm must implement private-key cryptography.
- The algorithm must be a block cipher.
- The algorithm must work on 128-bit blocks and support 3 keys sizes: 128, 192, and 256 bits.
- If selected, the algorithm should be available world-wide on a royalty-free basis

Description of AES

AES is an iterated cipher. The number of rounds (N) depends
on the key length: N = 10 for 128-bit keys, N = 12 for 192-bit keys, and N = 14 for 256-bit keys.
Here is a high-level description of AES:
1. Perform operation AddRoundKey, which XORs the round key with the state.
2. For each of the N rounds:
- perform operation ByteSub (a substitution using an S-box)
- perform operation ShiftRow (a permutation)
- perform operation MixColumn (unless it is the last round)
- perform AddRoundKey.

State:

All operations in AES are byte-based.
The state consists of 128 bits = 16 bytes, viewed as a 4x4 array of bytes.
Initially, the 16 bytes of plaintext x0, … , x15 are arranged as
follows:

X0	X4	X8	X12
X1	X5	X9	X13
X2	X6	X10	X14
X3	X7	X11	X16

ByteSub:

- operation performs a substitution on each byte
- uses one S-box that maps bytes to bytes.
- represented as a 16 x 16 array: for hexadecimal digits X and
Y, πS(XY) is at position (row X, column Y)

In contrast to the DES S-boxes, the AES S-box can be
defined algebraically. It was designed for resistance against
linear and differential cryptanalysis and it is invertible.
The AES box incorporates operations in the finite field with
28 elements:
GF(28) = Z2[X] (mod X8+X4+X3+X+1)

SHIFTROWS:

The ShiftRows stage provides a simple "permutation" of the data, whereas the other steps involve substitutions. Further, since the state is treated as a block of columns, it is this step which provides for diffusion of values between columns. It performs a circular rotate on each row of 0, 1, 2 & 3 places for respective rows. When decrypting it performs the circular shifts in the opposite direction for each row. This row shift moves an individual byte from one column to another, which is a linear distance of a multiple of 4 bytes, and ensures that the 4 bytes of one column are spread out to four different columns.

MIX COLUMN:

The forward mix column transformation, called MixColumns, operates on each column individually. Each byte of a column is mapped into a new value that is a function of all four bytes in that column. It is a substitution that makes use of arithmetic over GF(2^8). Each byte of a column is mapped into a new value that is a function of all four bytes in that column. It is designed as a matrix multiplication where each byte is treated as a polynomial in $GF(2^8)$. The inverse used for decryption involves a different set of constants.

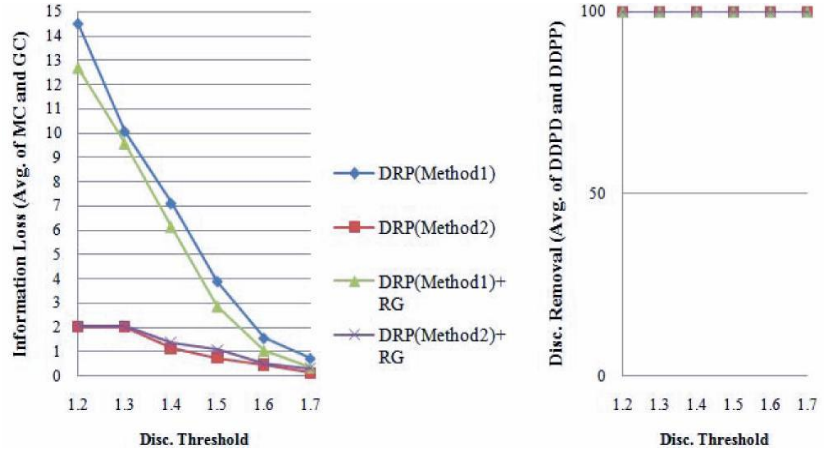
The constants used are based on a linear code with maximal distance between code words – this gives good mixing of the bytes within each column. Combined with the "shift rows" step provides good avalanche, so that within a few rounds, all output bits depend on all input bits.

E. Data Set

Adult data set : We used Adult data set. This data set consist 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 been 14 attributes. We used train part in our experiments. The data set contains both categorical and numerical attributes.

IV. RUSULT DISCUSSION

Fig.2 Left: Information loss,Right: Discrimination removal degree for [1.2,1.7]. DRP[DTM i]: Data transformation method I for DRP; RG: Rule Generalization Figure 2 shows at the left the degree of information loss (at the right the degree of discrimination removal (as average of DDPD and DDPP) of direct discrimination prevention methods for the Adult dataset when the value of the discriminatory threshold varies from 1.2 to 1.7, the minimum support is 5% and the minimum confidence is 10The number of direct discriminatory rules extracted from the dataset is 991 for =1.2, 415 for =1.3, 207 for =1.4, 120 for =1.5, 63 for =1.6 and 30 for =1.7 respectively



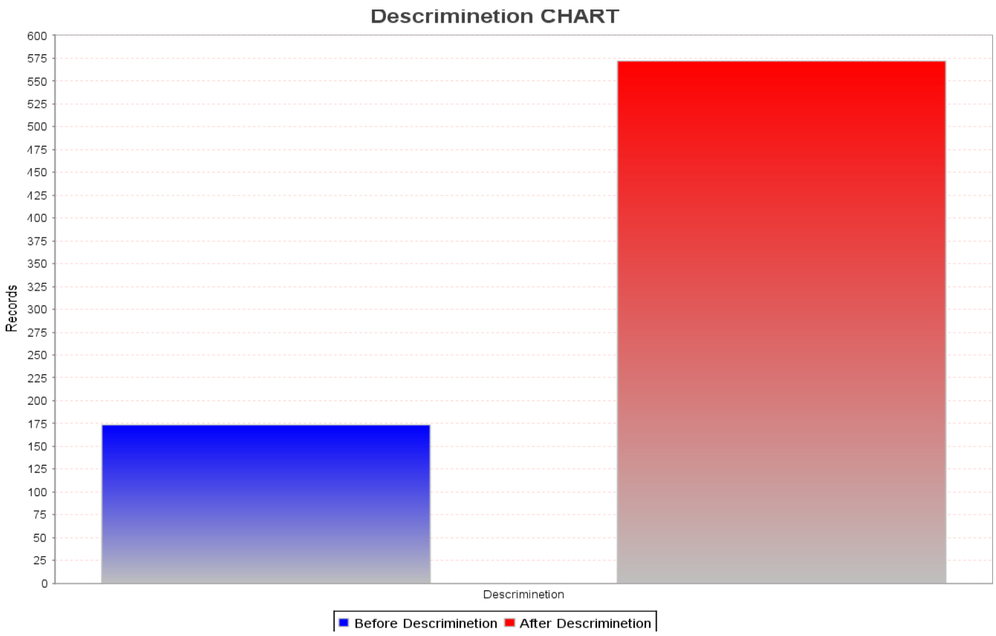


Fig.3 comparison between before discrimination and after discrimination removal

ADVANTAGES OF PROPOSED SYSTEM:

- Privacy-invasion
- Potential-discrimination
- Discrimination-Measurement
- Data Transformation

V. CONCLUSION

The purpose of this paper was to develop a new pre-processing discrimination prevention methodology including different data transformation methods that can prevent direct discrimination, indirect discrimination or both of them at the same time. To attain this objective, the first step is to measure discrimination and identify categories and groups of individuals that have been directly and/or indirectly discrimi-nated in the decision-making processes; the second step is to transform data in the proper way to remove all those discrim-inatory biases. Finally, discrimination-free data models can be produced from the transformed data set without seriously damaging data quality. Also Privacy preserving in data mining is done for security purpose. The experimental results reported demonstrate that the proposed techniques are quite successful in both goals of removing discrimination and preserving data quality

ACKNOWLEDGEMENT

This is a great pleasure & immense satisfaction to express my deepest sense of gratitude & thanks to everyone who has directly or indirectly helped me in my project work successfully.

I express my gratitude towards project guide **Prof.V.K.Bhusari**,and **Prof. G.M.Bhandari**, Head of Department of Computer Engineering , Bhivarabai Sawant Institute Of Technology and Research College Of Engineering, Pune who guided & encouraged me in my project work in scheduled time. I would like to thanks our **Principal Dr. D.M.Yadav**, for allowing us to pursue my project in this institute.

REFERENCES

[1] S. Hajian, J. Domingo-Ferrer, and A. Martı´nez-Balleste´, “Discrimination Prevention in Data Mining for Intrusion and Crime Detection,” Proc. IEEE Symp. Computational Intelligence in Cyber Security (CICS ’11), pp. 47-54, 2011.

[2] D. Pedreschi, S. Ruggieri, and F. Turini, “Discrimination-Aware Data Mining,” Proc. 14th ACM Int’l Conf. Knowledge Discovery and Data Mining (KDD ’08), pp. 560-568, 2008.

[4] R. Agrawal and R. Srikant, “Fast Algorithms for Mining Association Rules in Large Databases,” Proc. 20th Int’l Conf. Very Large Data Bases, pp. 487-499, 1994

[5] S. Hajian, J. Domingo-Ferrer, and A. Martı´nez-Balleste´, “Rule Protection for Indirect Discrimination Prevention in Data Mining,” Proc. Eighth Int’l Conf. Modeling Decisions for Artificial Intelligence (MDAI ’11), pp. 211-222, 2011

