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, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

An Improved Privacy Preserved Rule Mining for Credit Dataset with Discrimination Prevention

Boopathiraja K[1], Nithyakalyani S M.E., (Ph.D) [2]

Master of Technology, K.S.R. College of Engineering, Tamil Nadu, India[1]

Guide & Associate Professor, K.S.R. College of Engineering, Tamil Nadu, India[2]

ABSTRACT: Security and privacy methods are used to protect the data values. Private data values are secured with confidentiality and integrity methods. Privacy model hides the individual identity over the public data values. Sensitive attributes are protected using anonymity methods. Discrimination is the prejudicial treatment of an individual based on their membership in a certain group or category. Antidiscrimination acts are designed to prevent discrimination on the basis of a number of attributes in various settings. Public data collections are used to train association/classification rules in view of making automated decisions. Data mining can be both a source of discrimination and a means for discovering discrimination.

Automated data collection and data mining techniques such as classification rule mining are used to making automated decisions. Discriminations are divided into two types such as direct and indirect discriminations. Direct discrimination occurs when decisions are made based on sensitive attributes. Indirect discrimination occurs when decisions are made based on non sensitive attributes which are strongly correlated with biased sensitive ones. Discrimination discovery and prevention are used for anti-discrimination requirements. Direct and indirect discriminations prevention is applied on individually or both at the same time. The data values are cleaned to obtain direct and/or indirect discriminatory decision rules. Data transformation techniques are applied to prepare the data values for the discrimination prevention. Rule protection and rule generalization algorithm and direct and indirect discrimination prevention algorithm are used to protect discriminations.

The discrimination prevention model is integrated with the differential privacy scheme to high privacy. Dynamic policy selection based discrimination prevention is adopted to generalize the systems for all regions. Data transformation technique is improved to increase the utility rate. Discrimination removal process is improved with rule hiding techniques.

KEY WORDS—Discrimination, differential privacy, policy selection, rule protection, rule generalization

I. INTRODUCTION

Data mining and knowledge discovery in databases are two new research areas that investigate the automatic extraction of previously unknown patterns from large collections of data. Recent development in data collection, data dissemination and related technologies have inaugurated a new era of research where existing data mining algorithms should be reconsidered from a different point of view, this of privacy preservation. It is well documented that this new without limits explosion of new information through the Internet and other media, has reached to a point where threats against the privacy are very common on a daily basis and they deserve serious thinking.

Privacy preserving data mining, is a novel research direction in data mining and statistical databases, where data mining algorithms are analyzed for the side-effects they incur in data privacy. The main consideration in privacy preserving data mining is twofold. First, sensitive raw data like identifiers, gender, religion, addresses and the like should be changed or cut out from the original database, in order for the recipient of the data not to be able to compromise another person's

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, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

privacy. Second, sensitive data which can be mined from a database by using data mining algorithms should also be excluded, because such knowledge can equally well compromise data privacy. The main objective in privacy preserving data mining is to develop algorithms for changing the original data in some way, so that the private data and private knowledge remain private even after the mining process. The problem that arises when confidential information can be derived from released data by unauthorized users is also commonly called the "database inference" problem.

II. RELATED WORK

Despite the wide deployment of information systems based on data mining technology in decision making, the issue of antidiscrimination in data mining did not receive much attention until 2008 [9]. Some proposals are oriented to the discovery and measure of discrimination. Others deal with the prevention of discrimination.

The discovery of discriminatory decisions was first proposed by Pedreschi et al. [5]. The approach is based on mining classification rules (the inductive part) and reasoning on them (the deductive part) on the basis of quantitative measures of discrimination that formalize legal definitions of discrimination. For instance, the US Equal Pay Act states that: "a selection rate for any race, gender, or specific group which is less than four-fifths of the rate for the group with the highest rate will generally be regarded as evidence of adverse impact." This approach has been extended to encompass statistical significance of the extracted patterns of discrimination in [3] and to reason about affirmative action and favoritism [4]. Moreover it has been implemented as an Oracle-based tool in [6]. Current discrimination discovery methods consider each rule individually for measuring discrimination without considering other rules or the relation between them. However, in this paper we also take into account the relation between rules for discrimination discovery, based on the existence or nonexistence of discriminatory attributes.

Discrimination prevention, the other major antidiscrimination aim in data mining, consists of inducing patterns that do not lead to discriminatory decisions even if the original training data sets are biased. Three approaches are conceivable:

A. Preprocessing

Transform the original data in such a way that the discriminatory biases contained in the original data are completely trim so that no wrong decision rule can be mined from the transformed data and apply any of the standard data mining algorithms. The preprocessing approaches of data transformation and hierarchy-based generalization can be adapted from the privacy preservation literature. Along this line, [7], [8] perform a controlled distortion of the training data from which a classifier is learned by making minimally intrusive modifications leading to an unbiased data set. The preprocessing approach is useful for applications in which a data set should be published and/or in which data mining needs to be performed also by external parties

B. In processing

Change the data mining algorithms in such a way that the resulting models do not contain wrong decision rules. For example, an alternative approach to cleaning the discrimination from the original data set is proposed in [2] whereby the nondiscriminatory constraint is embedded into a decision tree learner by changing its splitting criterion and pruning strategy through a novel leaf relabeling approach. However, it is obvious that in processing discrimination prevention methods must rely on new special-purpose data mining algorithms; standard data mining algorithms cannot be used.

C. Post processing

Modify the resulting data mining models, instead of cleaning the original data set or changing the data mining algorithms. For example, in [3], a confidence-altering approach is proposed for classification rules inferred by the CPAR algorithm. The post processing approach does not allow the data set to be released: only the modified data mining models can be released (knowledge publishing), hence data mining can be performed by the data owner only.One might think of a straightforward preprocessing approach consisting of just removing the discriminatory attributes from the data set.

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, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Although this would solve the direct discrimination problem, it would cause much information loss and in general it would not solve indirect discrimination. As stated in [9] there may be other attributes (e.g., Zip) that are highly correlated with the sensitive ones (e.g., Race) and allow inferring discriminatory rules. Hence, there are two important challenges regarding discrimination prevention: one challenge is to consider both direct and indirect discrimination instead of only direct discrimination; the other challenge is to find a good tradeoff between discrimination removal and the quality of the resulting training data sets and data mining models.

Although some methods have already been proposed for each of the above-mentioned approaches (preprocessing, in-processing, post processing), discrimination prevention stays a largely unexplored research avenue. In this paper, we concentrate on discrimination prevention based on preprocessing, because the preprocessing approach seems the most flexible one: it does not require changing the standard data mining algorithms, unlike the in-processing approach, and it allows data releasing (rather than just knowledge is publishing), unlike the post-processing approach.

III. DISCRIMINATION PREVENTION SCHEMES

In sociology, discrimination is the prejudicial treatment of an individual based on their membership in a certain group or category. It involves rejecting to members of one group opportunities that are available to other groups. There is a list of antidiscrimination acts, which are laws designed to prevent discrimination on the basis of a number of attributes (e.g., race, religion, gender, nationality, disability, marital status, and age) in various settings (e.g., employment and job, access to public services, credit and finance, etc.).

Services in the information society allow for automatic and routine collection of large amounts 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, personnel selection, etc. At first sight, automating decisions may give a sense of fairness: classification rules do not guide themselves by personal preferences. However, at a closer look, one realizes that classification rules are actually learned by the system (e.g., loan acceptance) from the training data. If the training data are inherently biased for or against a particular community (e.g., black people), the learned model may show a discriminatory prejudiced behavior. In other words, the system may infer that just being black people is a legitimate reason for loan rejection. Discovering such potential biases and removing them from the training data without harming their decision making utility is therefore highly complex. One must prevent data mining from becoming itself a source of discrimination, due to data mining tasks generating discriminatory models from biased data sets as part of the automated decision making. In [9], it is demonstrated that data mining can be both a source of discrimination and a means for discovering discrimination.

Discrimination can be either direct or indirect (also called systematic). [1] Direct discrimination consists of rules or procedures that explicitly mention minority or specific group based on their sensitive discriminatory attributes related to group membership. Indirect discrimination consists of rules or procedures that, while not explicitly showing discriminatory attributes, intentionally or unintentionally could generate discriminatory decisions. Redlining by financial institutions (refusing to give mortgages or insurances in urban areas they consider as deteriorating) is an archetypal example of indirect discrimination, although certainly not the only one. With a slight abuse of culture and their membership for the sake of compactness, in this paper indirect discrimination will also be referred to as redlining and rules causing indirect discrimination will be called redlining rules [9]. Indirect discrimination could happen because of the availability of some background knowledge (rules), for example, that a certain zip code corresponds to a deteriorating area or an area with mostly black population. The background knowledge might be accessible from publicly available data (e.g., census data) or might be obtained from the original data set itself because of the existence of nondiscriminatory attributes that are highly correlated with the sensitive ones in the original data set. Discrimination prevention methods based on preprocessing published so far [7], [8] present some limitations, which we next highlight:

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, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

- They attempt to find discrimination in the original data only for one discriminatory item and based on a single measure. This approach cannot sure that the transformed data set is really discrimination free, because it is known that discriminatory behaviors can often be hidden inside several discriminatory items, and even behind combinations of them.
- They only consider direct discrimination.
- They do not obtain any measure to evaluate how much discrimination has been removed and how much information loss has been occurred.

IV. DISCRIMINATION PREVENTION ISSUES

Automated data acquisition and data mining techniques such as classification rule mining are used to making automated decisions. Discriminations are divided into two types such as direct and indirect discriminations. Direct discrimination occurs when decisions are made based on sensitive attributes. Indirect discrimination occurs when decisions are made based on insensitive attributes which are strongly correlated with biased sensitive ones. Discrimination discovery and prevention are used for anti-discrimination requirements. Direct and indirect discriminations prevention is applied on individually or both at the same time. The data values are cleaned to obtain direct and/or indirect discriminatory decision rules. Data transformation techniques are applied to prepare the data values for the discrimination prevention. Rule protection and rule generalization algorithm and direct and indirect discrimination prevention algorithm are used to protect discriminations. The following drawbacks are identified in the existing system.

- Static discrimination policy based scheme
- Limited utility ratio
- Low privacy assurance
- Privacy association is not analyzed

V. DIRECT AND INDIRECT DISCRIMINATION PREVENTION ALGORITHM

Algorithm 1 details our proposed data transformation method for simultaneous direct and indirect discrimination prevention. The algorithm starts with redlining rules. From each redlining rule ($r : X \rightarrow C$), more than one indirect α-discriminatory rule ($r' : A, B \rightarrow C$) might be generated because of two reasons: 1) existence of different ways to group the items in X into a context item set B and a nondiscriminatory item set D correlated to some discriminatory item set A; and 2) existence of more than one item in DI_s. Hence, as shown in Algorithm 4 (Step 5), given a redlining rule r, proper data transformation should be conducted for all indirect α-discriminatory rules $r' : (A \subseteq DI_s), (B \subseteq X) \rightarrow C$ ensuing from r.

Algorithm 1. Direct and Indirect Discrimination Prevention

1: Inputs: DB, FR, RR, MR, α, DI_s
2: Output: DB' (transformed data set)
3: for each $r : X \rightarrow C \in RR$, where $D,B \subseteq X$ do
4: $\gamma = conf(r)$
5: for each r' : $(A \subseteq DI_s), (B \subseteq X) \rightarrow C \in RR$ do
6: $\beta_2 = conf (r_{b2}: X \rightarrow A)$
7: $\Delta_1 = supp (r_{b2}: X \rightarrow A)$
8: $\delta = conf(B \rightarrow C)$
9: $\Delta_2 = supp (B \rightarrow A)$
10: $\beta_1 = \Delta_1/\Delta_2$ //$conf(r_{b1} : A,B \rightarrow D)$
11: Find DB_c: all records in DB that completely support $\neg A, B, \neg D \rightarrow \neg C$
12: Steps 6-9 Algorithm Direct Rule Protection (Method 1)
13: if r' $\in$ MR then

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, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

14:while ($\delta \leq \beta_1(\beta_{2+}\gamma\text{-}1)/\beta_2.\ \alpha$) and ($\delta \leq conf(r')/\alpha$) do
15: Select first record db_c in DB_c
16: Modify the class item of db_c from ¬C to C in DB
17: Recompute $\delta = conf(B \rightarrow C)$
18: end while
19: else
20: while $\delta \leq \beta_1(\beta_{2+}\gamma\text{-}1)/\beta_2.\ \alpha$ do
21: Steps 15-17 Algorithm Direct And Indirect Discrimination Prevention
22: end while
23: end if
24: end for
25: end for
26: for each r' : (A;B → C) 2 MR \ RR do
27: $\delta = conf\ (B \rightarrow C)$
28: Find DB_c: all records in DB that completely support ¬A,B→¬C
29: Step 12
30: while ($\delta \leq conf(r')/\alpha$) do
31: Steps 15-17 Algorithm Direct And Indirect discrimination Prevention
32: end while
33: end for
34: Output: DB' = DB

If some rules can be extracted from DB as both direct and indirect α-discriminatory rules, it means that there is overlap between MR and RR; in such case, data transformation is performed until both the direct and the indirect rule protection requirements are satisfied (Steps 13-18). This is possible because, the same data transformation method (Method 2 consisting of changing the class item) can provide both DRP and IRP. However, if there is no overlap between MR and RR, the data transformation is performed according to Method 2 for IRP, until the indirect discrimination prevention requirement is satisfied (Steps 19-23) for each indirect α-discriminatory rule ensuing from each redlining rule in RR, this can be done without any negative impact on direct discrimination prevention. Then, for each direct α-discriminatory rule r' Є MR\RR (that is only directly extracted from DB), data transformation for satisfying the direct discrimination prevention requirement is performed (Steps 26-33), based on Method 2 for DRP; this can be done without any negative impact on indirect discrimination prevention. Performing rule protection or generalization for each rule in MR by each of Algorithms 1-4 has no adverse effect on protection for other rules (i.e., rule protection at Step i + x to make r' protective cannot turn into discriminatory a rule r made protective at Step i) because of the two following reasons: the kind of data transformation for each rule is the same (change the discriminatory item set or the class item of records) and there are no two α-discriminatory rules r and r' in MR such that r = r'.

VI. PROPOSED WORK

The proposed discrimination prevention model is integrated with the differential privacy scheme to high privacy which means. Dynamic policy selection based discrimination prevention is adopted to generalize the systems for all regions. Data transformation technique is improved to increase the utility rate. Discrimination removal process is improved with rule hiding techniques by hiding sensitive rules.

The discrimination prevention system is designed to protect the decisions that are derived from the rule mining process. The system is divided into five major modules. They are data cleaning process, privacy preservation, rule mining, rule hiding and discrimination prevention.

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, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

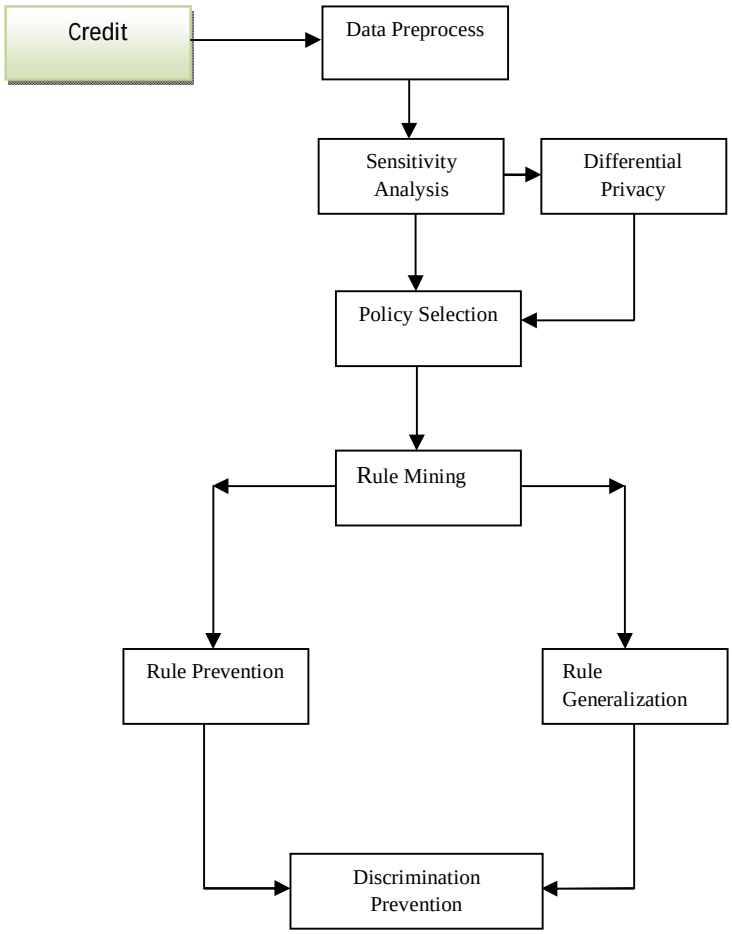

Figure 1: Overview of Proposed System

6.1 Differential Privacy to Data

A. Formal Definition

K gives e-differential privacy if for all values of DB, DB' differing in a single element, and all S in Range (*K)*

$$\frac{Pr[K(DB) \text{ in } S]}{Pr[K(DB') \text{ in } S]} \leq e^{\varepsilon} \sim (1+\varepsilon)$$

B. How to Achieve Differential Privacy

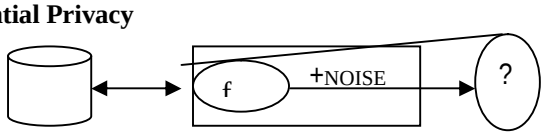

Figure 2: Achieving Differential Privacy

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, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

f: DB → R^d
K (f, DB) = f (DB) + [Noise]^d
E.g., Count (P, DB) = # rows in DB with Property P

C. How does it work?

$\Delta f = \max_{DB, DB\text{-}Me} |f(DB) - f(DB\text{-}Me)|$
Theorem: To achieve ε-differential privacy, use scaled symmetric noise Lap(R) with R = Δf/ε.

D. Example

ID	Claim ('000$)	ID	Claim ('000$)
1	9.91	7	10.63
2	9.16	8	12.54
3	10.59	9	9.29
4	11.27	10	8.92
5	10.50	**11**	**20**
6	11.89	12	8.55

Query: Average claim
Aux input: 12 entries
e = 1 → hide me among 1200 people
$\Delta f = \max_{DB, DB\text{-}Me} |f(DB) - f(DB\text{-}Me)|$
$= \max_{DB, DB\text{-}Me} |$ Avg (DB) – Avg (DB-Me)|
= 20-12.54 = 7.46→ max is a sensitive function!
Add noise: Lap(Df/e) = Lap(7.46/1) = Lap(7.46)

VII. OVERALL FUNCTIONALITIES OF PROPOSED MODEL

A. Data Cleaning Process

Data populate and missing value assignment operations are carried out in the data cleaning process. Textual data values are transferred into the Oracle database. Incomplete transactions are updated with alternate values. Aggregation based data substitution method is used for data assignment process.

B. Privacy Preservation

Privacy preservation is applied to protect sensitive attributes. Differential privacy technique is applied on sensitive attributes. Noise is added with the sensitive attributes. Data transformation process is applied to prepare the data for rule mining process.

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, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

C. Rule Mining

The rule mining process is performed to filter the frequent patterns. Candidate sets are prepared using attribute name and values. Support and confidence values are estimated using item sets. Frequent patterns are identified with minimum support and confidence values.

D .Rule Hiding

Rule hiding method is applied to protect the sensitive rules. Rules derived from sensitive attributes are not released directly. Rules are embedded with nearest rule intervals.

E. Discrimination Prevention

Discrimination prevention process is designed to protect decisions. Rule generalization and rule prevention algorithms are enhanced for dynamic policy model. Direct and indirect discrimination prevention algorithm is also tuned for dynamic policy scheme. Discriminations are protected with reference to sensitive and non-sensitive attributes.

VIII. CONCLUSION

Data mining techniques are applied to hidden knowledge from data bases. Discriminatory decisions are obtained and prevented with reference to the attributes. Direct and indirect discrimination prevention scheme is used to protect the decision rules. The discrimination prevention scheme is enhanced with dynamic policy selection model and differential privacy mechanisms. The system increases the data utility rate. Policy selection based discrimination prevention model can be applied for all regions. Privacy preserved rate is improved by the system. Rule privacy is optimized with rule generalization mechanism.

REFERENCES

[1] 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.
[2] T. Calders and S. Verwer, "Three Naive Bayes Approaches for Discrimination-Free Classification," Data Mining and Knowledge Discovery, vol. 21, no. 2, pp. 277-292, 2010.
[3] D. Pedreschi, S. Ruggieri, and F. Turini, "Measuring Discrimination in Socially-Sensitive Decision Records," Proc. Ninth SIAM Data Mining Conf. (SDM '09), pp. 581-592, 2009.
[4] D. Pedreschi, S. Ruggieri, and F. Turini, "Integrating Induction and Deduction for Finding Evidence of Discrimination," Proc. 12th ACM Int'l Conf. Artificial Intelligence and Law (ICAIL '09), pp. 157-166, 2009.
[5] S. Ruggieri, D. Pedreschi, and F. Turini, "Data Mining for Discrimination Discovery," ACM Trans. Knowledge Discovery from Data, vol. 4, no. 2, article 9, 2010.
[6] S. Ruggieri, D. Pedreschi, and F. Turini, "DCUBE: Discrimination Discovery in Databases," Proc. ACM Int'l Conf. Management of Data (SIGMOD '10), pp. 1127-1130, 2010.
[7] F. Kamiran and T. Calders, "Classification without Discrimination," Proc. IEEE Second Int'l Conf. Computer, Control and Comm. (IC4 '09), 2009.
[8] F. Kamiran and T. Calders, "Classification with no Discrimination by Preferential Sampling," Proc. 19th Machine Learning Conf. Belgium and The Netherlands, 2010.
[9] 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.560-568,008.