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

Decision Prevention Mechanism for Frequent Pattern Mining Process

L. Gomathi[1], Mr. A.T. Ravi, ME (Ph.D) [2]

II-M.E (CSE), Dept. of CSE, SSM College of Engineering, Komarapalayam, Tamilnadu, India[1]

Assistant Professor, Dept. of CSE, SSM College of Engineering, Komarapalayam, Tamilnadu, 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.

I. INTRODUCTION

Automated data collection in the information society facilitates automating decision making as well. Superficially, 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 trained on the collected data. If those training data are biased, the learned model will be biased. For example, if the data are used to train classification rules for loan granting and most of the Brazilians in the training dataset were denied their loans, the leaned rules will also show biased behavior toward Brazilian and it is a discriminatory reason for loan denial. Unfairly treating people on the basis of their belonging to a specific group is known as discrimination and is legally punished in many democratic countries.

The literature in law and social sciences distinguishes direct and indirect discrimination. Direct discrimination consists of rules or procedures that explicitly impose "disproportionate burdens" on minority or disadvantaged groups based on sensitive attributes related to group membership [9]. Indirect discrimination consists of rules or procedures that, while not explicitly mentioning discriminatory attributes, impose the same disproportionate burdens, intentionally or unintentionally. This effect and its exploitation is often referred to as redlining and indirectly discriminating rules can be called redlining rules. The term "redlining" was invented in the late 1960s by community activists in Chicago. The authors

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

also support this claim: even after removing the discriminatory attributes from the dataset, discrimination persists because there may be other attributes that are highly correlated with the sensitive ones or there may be background knowledge from publicly available data allowing inference of the discriminatory knowledge.

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. 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, sex, or ethnic 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 [1] and to reason about affirmative action and favoritism [6]. Moreover it has been implemented as an Oracle-based tool in [4]. 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: Preprocessing. Transform the source data in such a way that the discriminatory biases contained in the original data are removed so that no unfair 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, [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.

In-processing. Change the data mining algorithms in such a way that the resulting models do not contain unfair 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. Postprocessing. Modify the resulting data mining models, instead of cleaning the original data set or changing the data mining algorithms. For example, a confidence-altering approach is proposed for classification rules inferred by the CPAR algorithm. The postprocessing approach does not allow the data set to be published: only the modified data mining models can be published, hence data mining can be performed by the data holder only.

One might think of a straightforward preprocessing approach consisting of just removing the discriminatory attributes from the data set. 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 [3] there may be other attributes that are highly correlated with the sensitive ones 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, discrimination prevention stays a largely unexplored research avenue. In this paper, we concentrate on discrimination prevention based on preprocessing.

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

III. SECURITY FOR DISCRIMINATIONS

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 from the training data. If the training data are inherently biased for or against a particular community, the learned model may show a discriminatory prejudiced behavior. In other words, the system may infer that just being foreign is a legitimate reason for loan denial. Discovering such potential biases and eliminating them from the training data without harming their decision making utility is therefore highly desirable. 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 [3], 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. Direct discrimination consists of rules or procedures that explicitly mention minority or disadvantaged groups based on sensitive discriminatory attributes related to group membership. Indirect discrimination consists of rules or procedures that, while not explicitly mentioning discriminatory attributes, intentionally or unintentionally could generate discriminatory decisions. Redlining by financial institutions is an archetypal example of indirect discrimination, although certainly not the only one. With a slight abuse of language 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. Indirect discrimination could happen because of the availability of some background knowledge, 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 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] present some limitations, which we next highlight: They attempt to detect discrimination in the original data only for one discriminatory item and based on a single measure. This approach cannot guarantee that the transformed data set is really discrimination free, because it is known that discriminatory behaviors can often be hidden behind several discriminatory items, and even behind combinations of them. They only consider direct discrimination. They do not include any measure to evaluate how much discrimination has been removed and how much information loss has been incurred. In this system propose preprocessing methods which overcome the above limitations. Our new data transformation methods are based on measures for both direct and indirect discrimination and can deal with several discriminatory items. Also, we provide utility measures. Hence, our approach to discrimination prevention is broader than in previous work.

In our earlier work introduced the initial idea of using rule protection and rule generalization for direct discrimination prevention, but we gave no experimental results. We introduced the use of rule protection in a different way for indirect discrimination prevention and we gave some preliminary experimental results. In this paper, we present a unified approach to direct and indirect discrimination prevention, with finalized algorithms and all possible data transformation methods based on rule protection and/ or rule generalization that could be applied for direct or indirect discrimination prevention. We specify the different features of each method. Since methods in our earlier papers could only deal with either direct or indirect discrimination, the methods described in this paper are new.

IV. PROBLEM STATEMENT

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

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

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 following drawbacks are identified in the existing system. They are static discrimination policy based scheme, limited utility ratio low privacy assurance and privacy association is not analyzed.

V. DECISION PREVENTION FOR FREQUENT PATTERN MINING

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. The discrimination prevention system is designed to protect the decisions that are derived from the rule mining process. The system is enhanced to improve the data utility rate and privacy preservation rate. Policy selection model is used to perform dynamic policy based discrimination prevention tasks. The system is divided into five major modules. They are data cleaning process, privacy preservation, rule mining, rule hiding and discrimination prevention. The data cleaning module is designed to prepare the data for mining process. Privacy preservation module is designed to protect sensitive attribute. Frequent pattern mining operations are performed under the rule mining module. Sensitive rules are protected under the rule hiding process. Discrimination prevention module is used to perform direct and indirect discrimination prevention process.

5.1. 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. The proposed solution to prevent direct discrimination is based on the fact that the data set of decision rules would be free of direct discrimination if it only contained PD rules that are α-protective or are instances of at least one nonredlining PND rule. Therefore, a suitable data transformation with minimum information loss should be applied in such a way that each α-discriminatory rule either becomes α-protective or an instance of a nonredlining PND rule. We call the first procedure direct rule protection (DRP) and the second one rule generalization.

The proposed solution to prevent indirect discrimination is based on the fact that the data set of decision rules would be free of indirect discrimination if it contained no redlining rules. To achieve this, a suitable data transformation with minimum information loss should be applied in such a way that redlining rules are converted to nonredlining rules. We call this procedure indirect rule protection (IRP).

5.2. 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. Differential privacy is a recent privacy definition that guarantees the outcome of a calculation to be insensitive to any particular record in the data set. The parameter $\in$ allows us to control the level of privacy. Lower values of $\in$ mean stronger privacy, as they limit further the inuence of a record on the outcome of a calculation. The values typically considered for $\in$ are smaller than 1, e.g., 0.01 or 0.1. The definition of differential privacy maintains a composability property: when consecutive queries are executed and each maintains differential privacy, their $\in$ parameters

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

can be accumulated to provide a differential privacy bound over all the queries. Therefore, the ϵ parameter can be treated as a privacy cost incurred when executing the query.

These costs add up as more queries are executed, until they reach an allotted bound set by the data provider, at which point further access to the database will be blocked. The composition property also provides some protection from collusion: collusion between adversaries will not lead to a direct breach in privacy, but rather cause it to degrade gracefully as more adversaries collude, and the data provider can also bound the overall privacy budget. Typically, differential privacy is achieved by adding noise to the outcome of a query. One way to do so is by calibrating the magnitude of noise required to obtain ϵ-differential privacy according to the sensitivity of a function. The sensitivity of a real-valued function expresses the maximal possible change in its value due to the addition or removal of a single record.

5.3. 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. A number of data mining algorithms have been recently developed that greatly facilitate the processing and interpreting of large stores of data. One example is the association rule-mining algorithm, which discovers correlations between items in transactional databases. Priori algorithm is an example of association rule mining algorithm. Using this algorithm, candidate patterns that receive sufficient support from the database are considered for transformation into a rule. This type of algorithm works well for complete data with discrete values. One limitation of many association rule-mining algorithms such as the Apriori algorithm is that only database entries, which exactly match the candidate patterns, may contribute to the support of the candidate pattern. This creates a problem for databases containing many small variations between similar patterns and for databases containing missing values.

A number of data mining algorithms have been introduced to the community that perform summarization of the data, classification of data with respect to a target attribute, deviation detection and other forms of data characterization and interpretation. One popular summarization and pattern extraction algorithm is the association rule algorithm, which identifies correlations between items in transactional databases. Given a set of transactions, each described by an unordered set of items, an association rule $X - Y$ may be discovered in the data, where X and Y are conjunctions of items. The intuitive meaning of such a rule is that transactions in the database, which contain the items in X, tend to also contain the items in Y.

5.4. 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. Attribute ranges are adjusted with sensitive rules. The hiding strategies, that we propose, heavily depend on finding transactions that fully or partially support the generating itemsets of a rule. The reason for this is that if we want to hide a rule, we need to change the support of some part of the rule. Another issue is that the changes in the database introduced by the hiding process should be limited, in such a way that the information loss incurred by the process is minimal. According to this, we try to apply minimal changes in the database at every step of the hiding algorithms that we propose.

The decrease in the support of an itemset *S* can be done by selecting a transaction *t*, that supports *S* and by setting to 0 at least one of the non-zero values of *t.values of items* that represent items in *S*. The increase in the support of an itemset *S* can be accomplished by selecting a transaction *t* that partially supports it and setting to 1 the values of all the items of *S* in *t. values of items*. In order to be able to identify some viable ways for reducing either the support or the confidence of a rule, we need to analyze the formulas that we have already presented for the confidence and the support. Both the confidence and the support are expressed as ratios of supports of itemsets that support the two parts of a rule or its generating itemset. In this way, if we want to lower the value of a ratio, we can adopt either one of the following options:

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

(a) we can decrease the numerator, while keeping the denominator fixed, or (b) we can increase the denominator while keeping the numerator fixed.

5.5. 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. The qualitative statements in existing laws, regulations, and legal cases into quantitative formal counterparts over classification rules and they introduced a family of measures of the degree of discrimination of a PD rule. One of these measures is the extended lift (elift).

The idea here is to evaluate the discrimination of a rule as the gain of confidence due to the presence of the discriminatory items (i.e., A) in the premise of the rule. Whether the rule is to be considered discriminatory can be assessed by thresholding elift. The purpose of direct discrimination discovery is to identify α-discriminatory rules. In fact, α–discriminatory rules indicate biased rules that are directly inferred from discriminatory items. We call these rules direct α-discriminatory rules. In addition to elift, two other measures slift and olift were proposed by Pedreschi et al. The reason is that different measures of discriminating power of the mined decision rules can be defined, according to the various antidiscrimination regulations in different countries. Yet the protection methods are similar no matter the measure adopted.

The purpose of indirect discrimination discovery is to identify redlining rules. In fact, redlining rules indicate biased rules that are indirectly inferred from nondiscriminatory items because of their correlation with discriminatory ones. To determine the redlining rules stated the theorem below which gives a lower bound for α-discrimination of PD classification rules, given information available in PND rules (γ,δ), and information available from background rules (β_1, β_2). They assume that background knowledge takes the form of classification rules relating a nondiscriminatory item set D to a discriminatory item set A within the context B.

VI. 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] 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.

[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, "Discrimination-Aware Data Mining," Proc. 14th ACM Int'l Conf. Knowledge Discovery and Data Mining (KDD '08), pp. 560-568, 2008.

[4] 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.

[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.

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

[6] 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.

[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] 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.