Discrimination Resistant Privacy Preserved Data Mining

Anju Sundaresan, Lakshmi S

Abstract— These Data mining is the process of analyzing and summarizing data and extracting some useful information. There are some negative issues related to data mining. Potential discrimination and potential privacy invasion are two important issues among them. Discrimination is the phenomenon of unfairly treating people based on their membership in some group or category. Automated data collection may lead the way to making automated decisions, like loan granting/denial, insurance premium computation, job granting/denial etc. So, antidiscrimination techniques such as discrimination discovery and prevention have been introduced in data mining. Mainly there are two types of discrimination, direct discrimination and indirect discrimination. Privacy Preserving Data Mining deals with protecting the privacy of individual data or sensitive knowledge. There are no studies developed yet to avoid discrimination and privacy invasion simultaneously. In this work, to avoid these issues the following methods are combined. The basic idea behind discrimination finding is to apply the rule mining algorithms on the given datasets. The measure of impact of the rules is found out using elift function; the measure may be used in algorithms for prevention of direct and indirect discrimination. A discriminative attribute may be protected using two methods- direct rule protection and rule generalization algorithms. Privacy preservation is carried out based on K anonymity algorithm. In K anonymity attributes are suppressed or generalized until each row is identical with at least k-1 other rows.

Index Terms— Discrimination, Privacy Preservation, K Anonymity,Rule protection, sensitive attribute

1 INTRODUCTION

Nowadays, large amount of personal data is stored by individuals or organizations. Privacy of those data is important. So, privacy preserving data mining is now a popular research area. Privacy Preserving Data Mining mainly looks for some methods to alter the original data in such a way that information determined from the altered data are close to original and the privacy of users is not falling out. There are so many methods proposed to avoid privacy invasion. Main drawbacks of these methods are information loss and reduction in data utility, decrease the efficiency of data mining. Another issue that relate to data mining is potential discrimination. Discrimination is the process of unfairly treating people based on their group or category. In this work a technique is proposed which avoid both potential privacy invasion and potential discrimination.

Now we have big opportunities of sensing, storing and analyzing data on human activities at detail. For example, the mobile devices can record the traces of our movements and search engines record all logs of our queries for obtaining sensitive information on the internet Data analysis and data mining techniques support knowledge discovery from human activity data to improve the quality of on-line and off-line services for users and also they are increasingly raising user privacy concerns on the other side. From the user's point of view, insufficient privacy protections on the part of a service they use would cause personal or sensitive information retrieval by a hacker. In order to respond to the above challenges, data privacy preservation technology needs to be developed in simultaneously with data mining and publishing techniques.

Discrimination refers to an unjustified treatment of any person based on their physical or cultural environment such as sex, age religion etc. Nowadays socially sensitive decisions may be taken by automatic systems such as loan granting or denial, job application, school admission etc. So data mining and data analytics on data about people must understand many ethical values not only data protection but also non-discrimination. Discrimination prevention in data mining (DPDM) promises high quality data which avoid the conflict between non-discrimination and data/model utility.

In this work, by identifying the problem related to privacy invasion and potential discrimination, it is realized that both of them are intertwined concept. That is, both of them share some common problems and common challenges. This work aims to find a new way to avoid these challenges simultaneously.

2 RELATED WORK

There are so many authors' present different methods to avoid discrimination in data mining. The analysis and limitations of these methods are given below.

T. Calders and S. Verwer[6] suggest two Naïve Bayes approach for discrimination resistant data base. This technique is to avoid dependence among attributes by removing correlation between sensitive attributes and other attributes. This data set is used to train Naïve Bayes classifier. In this model there is lowest dependence on sensitive attribute resulting only 5% of discrimination. Main limitations of this technique is that it is not suitable for indirect discrimination and the low accuracy of data.

F. Kamiran [7] use a method of preferential sampling for discrimination free classification. They propose an idea of classification with no discrimination. It makes changes to the distribution of different data objects using preferential sampling techniques to make it discrimination free. It is a preprocessing discrimination prevention method. This method is based on some ranking algorithm. Low data rate and minimum discrimination removal are the main drawback of this method.

Discrimination Discovery in Databases by Turini et al.[8] suggest DCUBE is a tool which detect discrimination through interactive and iterative processes. The main idea behind this tool is classification rule extraction. This tool also provides some knowledge to users about discrimination facts in a user friendly manner. The future users of DCUBE include: antidiscrimination establishment, proprietors of socially susceptible decision databases, and researchers, auditors in social sciences, economics and law.

S. Hajian et al.[9] proposed a new pre-processing approach for indirect discrimination prevention. This approach is based on data transformation. It is based on several discriminatory attribute and their combinations. This technique uses some measures to evaluating this. This is the first approach that uses a discrimination prevention method for indirect discrimination. In order to prevent indirect discrimination in the training dataset, first step consists in discovering indirect discrimination.

If any discrimination is found, the original training dataset is modified until discrimination is brought below a certain threshold or is entirely eradicated. It aims at generating training data which are free or almost free from indirect discrimination while preserving their usefulness to data mining algorithms. This approach can deal with only indirect discrimination. Application areas: Credit assessment, financial institution, insurance companies.

Sara Hajian and Josep Domingo-Ferre [1] suggest direct and indirect discrimination prevention method. This method is suitable for both direct and indirect discrimination. Direct discrimination is the process of treating people unfairly which is based on their cast, age, religion, qualification etc. in the case of indirect discrimination which occur when take decisions based on non sensitive attribute which is more related with sensitive attribute. It can be done individually or both at same time. This method mainly consists of two phases, discrimination measurement and data transformation. The main drawback of this method is that it doesn't deal with any privacy preservation technique.

Charu C. Aggarwal [3] suggests K anonymity method of data protection. This method is used to mask exact value of the attribute. The perturbation technique based on K-Anonymity was suitable for individual distribution aggregation. It is a post processing approach.

There is no study developed to achieve discrimination prevention and privacy preservation simultaneously. This paper combine the technique based on privacy preservation using K-anonymity [2] and discrimination prevention using direct and indirect discrimination prevention method [1].

3 PROPOSED SYSTEM

Proposed system uses two data transform methods rule protection and K anonymity. In design, find out the discrimination measure first. Apriori based rule mining algorithm is used to find the entire association rule present in the data set. Figure 1 shows overall architecture of the system.

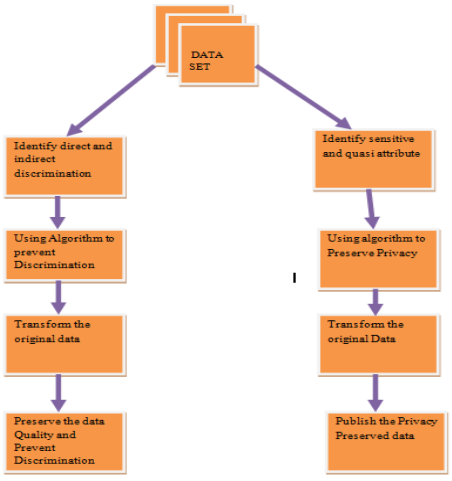

Figure 1.System Architecture

- *Anju Sundaresan is currently pursuing masters degree program in computer science and engineering in University of Kerala, IndiaE-mail: anjusnov91@mail.com*
- *Lakshmi S is currently pursuing Assistant Professor in computer science and engineering in University of Kerala, India, E-mail: lakshmi.rnath@gmail.com*

3.1 Discriminatory And Non Discriminatory Classification Rule

Let I be some discriminatory item set in our data set. For example I= {Age=36, Race =White, Gender = Male}. A classification rule Y→C is called potentially discriminatory when Y is an instance of discriminatory item set.

A classification rule Y→C is called non discriminatory if Y is not an instance of discriminatory item set. Figure 2 shows Rule mining for discrimination prevention.

Figure 2. Rule Mining

3.2 Direct Discrimination Measurement

Pedreschi et al. [12], suggest some measures for discrimination. Extended lift (elift) is one among them. Let A,B → C be a classification rule such that conf(A,B→C)> 0 then

$$elift(A,B \rightarrow C) = \frac{conf(A,B \rightarrow C)}{conf(B \rightarrow C)}$$

If elift of a rule is greater than some threshold, then it is discriminatory. Figure 3 shows Direct Discrimination Measurement and Prevention.

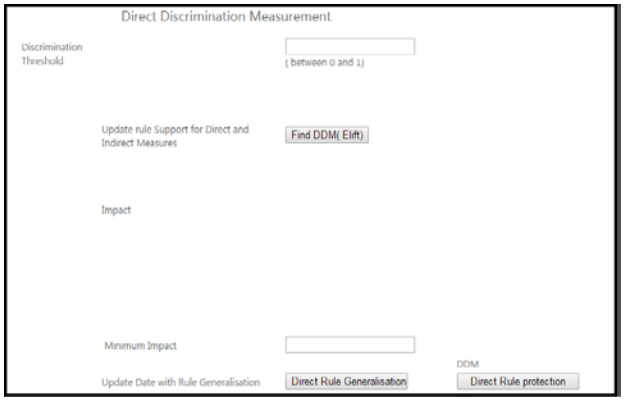

Figure 3: Direct Discrimination Measurement and Prevention

3.3 Indirect Discrimination Measurement.

Aim of indirect discrimination measurement is to avoid redlining rule. It is obtained from potentially non discriminatory rules and some back ground rules.

Let $r1 = D, B \rightarrow C$ be PND rule and

$$\gamma = conf(r1)\delta = conf(B \rightarrow C) > 0$$

Let A be a discriminatory item set, and let β_1, β_2 such that

$$conf(A, B \rightarrow D) \geq \beta_1$$

$$conf(D, B \rightarrow A) \geq \beta_2 > 0$$

$$f(x) = \frac{\beta_1}{\beta_2}(\beta_2 + x - 1)$$

$$elb(x,y) = \begin{cases} f(x)/y \ if \ f(x) > 0 \\ 0 \ otherwise \end{cases}$$

If $elb(\gamma, \delta) \geq \alpha$ then the PD classification rule is α discriminatory. Figure 4 shows Indirect Discrimination Measurement and Prevention.

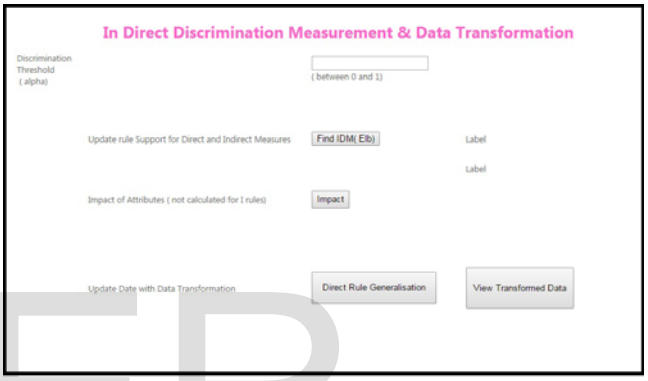

Figure 4 : Indirect Discrimination Measurement and Prevention.

3.4 Direct Rule Protection Algorithm

Let Db be the original database, Fr be the set of Frequent rule, Mr be a set of Measured rules and I be the discriminatory item set.

1. Input: Db,Fr,Mr,α,I
2. Output: Transformed data set(Db')
3. for each $r' : A, B \rightarrow C \in Mr$ do
4. for each $db_c \in Db$
5. compute impact(db_c)
6. end for
7. sort Db in ascending order of impact
8. while $conf(r') > \alpha . conf(B \rightarrow C)$
9. Modify discriminatory item set A of db_c

Output Db'=Db

3.5 Direct Rule Generalization Algorithm

1. Input: DB,MR,p=0.8,α,
2. Output : DB'
3. For each discriminatory rules r':A,B→C
4. Find the impact of each attribute present in the rule
5. Arrange in the ascending order of impact
6. While $conf(r') > \frac{conf(D, B \rightarrow C)}{p}$ do
7. Select first record in DB
8. modify the attribute C
9. Recompute conf(r')

3.6 Indirect Rule Generalaization Algorithm

1. Input: DB,RR,α,DIs
2. Output: DB'
3. for each rule r: X→C d
4. γ =conf(r)
5. for each r': (A DIs),(B X)→C
6. $\beta 2$=conf(X→A), $\Delta 1$ =Supp(X→A),
7. δ= conf(B→C) and $\beta 1 = \frac{\Delta_1}{\Delta_2}$
8. Compute the impact of each attribute
9. while $\gamma \geq \frac{\propto . \delta . \beta_2}{\beta_1}$
10. Modify the non discriminatory item set

3.7 Privacy Preservation using K Anonymity

One of the efficient methods to achieve privacy in data mining is K Anonymity. K Anonymity protects against identity disclosure rather than attribute disclosure. Table 1.1 shows two anonymous view of a data set.

Id	Zipcode	Age	Gender	Diagnostic
1	423***	>25	M	Flu
2	423***	>25	M	Flu
3	4236**	3*	F	Cancer
4	4236**	3*	F	Cancer
5	428***	>40	*	HIV
6	428***	>40	*	HIV

Table 1.1 Two Anonymous view of Data Set

In this work, K Anonymity model used to protect sensitive attribute. Some attribute value must keep secret by each individual called sensitive attribute. The traditional model takes all record from the original data set and processes it. There will be a loss of lot of information. This method select high sensitive record and other records published directly. Fig 2 shows the working of K anonymity model.

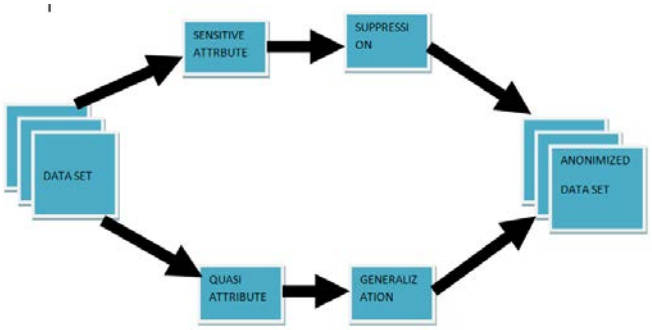

Figure 5. Anonimization

1. *Key Attribute*

Most unique attribute contained in the data set is called Key attribute. This attribute is mainly used to identify a record. For example Social Security Number, Name etc.

2. *Quasi Identifier*

Non sensitive attribute present in the data set is called Quasi identifier. This identifier is also called Candidate key. Quasi identifier Cannot be removed from micro data.

3. *Sensitive Attribute*

Sensitive attribute are the attribute which needs to be protected. Example: Account number.

This system anonymize only the most Sensitive attributes and quasi attributes to increase the data utility. Algorithm for anonimization is given below.

Algorithm

1. Input: Database D, Quasi Attribute, Sensitive Attribute
2. Output: Releasing database
3. Select Dataset D
4. Select Quazi-identifier attribute and Sensitive Attribute from give n attribute list.
5. Apply Suppression technique to most sensitive attribute

6. Apply Generalization technique to selected quasi attribute
7. Release Database

4 CONCLUSION

The proposed system focused to avoid two negative issues relates to data mining that is Potential Discrimination and Privacy invasion. This paper suggests some methods to avoid these two issues simultaneously. These technique applies rule protection and rule generalization technique to prevent discrimination and K Anonimization technique to achieve privacy in data. In Rule and rule generalization method change an item set which shows discriminatory behavior and have low impact to the data set. In K Anonimization, use suppression and generalization technique to preserve privacy.

Present system is capable of managing discrimination prevention by separate algorithms for direct and indirect discrimination In future a single algorithm can be developed, by eliminating the separation of methods. The method may depend upon some measurement that may suit to direct and indirect discrimination. Also the method of privacy preservation is now focused with data hiding up to a large level , it may tend to a generalization level protection in future. This can also be done in a single protection algorithm.

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]. 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.

[3]. Charu C. Aggarwal, (2005), ''On k-Anonymity and the Curse of Dimensionality", Proceedings of the 31st VLDB Conference, Trondheim, Norway, pp.901-909.

[4]. Ashwin Machanavajjhala , Daniel Kifer,Johannes Gehrke, Muthuramakrishnan Venkita Subramanian, (2006)," ℓ-Diversity : Privacy Beyond K-Anonymity", Proc.International conference on Data Engineering.(ICDE),pp.24.

[5]. Anil Prakash, Ravindar Mogili ,(2012),''Privacy Preservation Measure using t-closeness with combined l-diversity and k-anonymity", International Journal of Advanced Research in Computer Science and Electronics Engineering (IJARC SEE)Volume 1, Issue 8,pp:28-33

[6]. 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

[7]. F. Kamiran and T. Calders, "Classification with no Discrimination by Preferential Sampling," Proc. 19th Machine Learning Conf. Belgium and The Netherlands, 2010

[8]. 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.

[9]. S. Hajian, J. Domingo-Ferrer, and A. Martinez-Balleste, Rule protection for indirect discrimination prevention in data mining," in Modeling Decision for Artificial Intelligence, pp. 211-222, Springer, 2011.