Approach to Filter Transaction Risk Based on Distance Discriminant

Zheng Yu-Wei[1,2],
1. Department of Electronics and Information Engineering,
Tongji University, Shanghai 201804, China;

Ding Zhi-Jun[1,2,+],
2. The Key Laboratory of Embedded System and Service Computing,
Ministry of Education, Tongji University, Shanghai 200092, China;

Xu Xiao-Feng[3]
3. Department of Economic Information Engineering,
Southwest University of Finance and Economics,
Chengdu Sichuan 611130, China)

Abstract: **With the growth of e-commerce payment requirements, electronic payments develop rapidly, but it also faces the problem of transaction risk brought by fraud and other reasons. Therefore it is very necessary to establish a transaction risk control system. There are a lot of fraud detection methods based on data mining models, but because of the imbalance samples problem it will easily lead to misclassification, thus normal user transactions is disturbed and resulting in the loss of transaction and other problems. This paper presents a method to build risk filter model for electronic transaction. This method is used for filtering the normal transaction before the strict model validation, reducing the burden of subsequent validation, raising the success rate of normal transactions and the response speed of the normal transactions. This paper provides a distance discrimination method to judge filter conditions and conduct an experiment on the massive real transaction data. The experimental results show that the method has a good effect of filtering normal transaction.**

Key words: Distance discrimination; transaction risk; risk filter; fraud detection; electronic payment security

1 INTRODUCTION

With the online payment demand of e-commerce, electronic payments develop rapidly. Because of the open Internet environment, online payments are facing the transaction risk brought by fraud and security problem. At present, more effective solutions to solve the transaction risk problem in industry are based on rules and data mining models. Rules are highly based on domain knowledge, so its recognition accuracy rate of fraud is very high, but rules are usually hard-coded and the types of fraud which rules can detect are limited[1]. Data mining models are more flexible, models such as C4.5 decision tree, logistic regression have been widely used[2]. However, the amount of transaction logs the e-commerce company produced everyday are very huge, but the fraud transactions are just tiny part of it. Applications of data mining models on transaction risk detection are faced with the problem of serious imbalanced sample [3]. Such problem often leads to poor performance of classification model. In order to reduce the financial losses, online payment companies tend to adopt a conservative strategy, making the model more stringent which can detect more fraud while lead to a high false positive rate.

Currently the stringent risk authentication of transaction is likely to cause a higher false positive rate and worse user experience, which directly leads to a lot of false positives transactions due to the large amount of transactions. When a transaction is identified as a risk, the system will send confirmation by SMS, e-mail or manual methods like telephone to confirm the transaction, which requires company to pay a large amount of additional communications and labor costs. Furthermore, the additional confirmation make users concern about security of electronic payment, disturb user's normal payment business process, and easily lead to failure of user's payment operation. Therefore, how to reduce interference to normal users under existing risk control system is a very essential research question.

This paper proposes a transaction filtering method which will verify normal electronic transactions before the strict model verification to solve the drawbacks of the simple model validation. If a transaction is verified as a normal trade, this transaction will be directly passed by the risk control system, otherwise it will be rechecked by strict model. Note that this method is just a measure of normal transaction, the transactions cannot be passed by the filtering method will also contains normal transaction and need to be classified by stringent model. Transaction filtering method and stringent model form the two levels risk control system. Through two levels of risk control the system will achieve a high abnormal transaction detection rate and low interference rate to normal transaction. The architecture diagram of risk control system based on two levels of risk control is shown by figure 1.

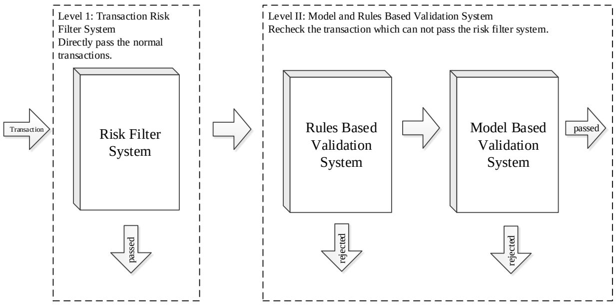

Figure 1 architecture diagram of risk control system based on transaction risk filter system

The rest of this paper is organized as follows: Section 2 gives a review about the current research on risk control of online transaction. Section 3 gives the details of transaction risk filtering model and describes the method to judge if a transaction reaches the filter conditions based on distance discrimination. Section 4 gives the experiment result on real transaction data and a short discussion about the result, and Section 5 concludes the study.

2 RELATED WORK

The researches on the transaction risk control currently focus on fraud detection, and most studies focus on applying the classification model to classify the normal and abnormal transactions, such as neural networks[4,5], decision tree[5], logistic regression[6], hidden Markov model[7]. Halvaiee has applied the artificial immune system to detect the fraud transactions[8]. But as Phua C[2] says, the experimental data set of most fraud detection research are not as large as the actual environment, and the imbalanced sample problem is not obvious in these data set while the proportion of fraud transactions is much lower in the real environment. Solving fraud detection with classification model are faced with the extreme imbalanced sample problem in real transactions data. Depending on selection of threshold, the classification model will have a problem of high false positive rate or low recall rate. So just applying classification model cannot properly solve the problem of fraud detection in e-commerce environment.

In this paper, in order to filter normal transaction, we want to build a method to measure the reliability of transactions. There are some studies to establish the trust mechanism for uses and transaction in electronic environment. Liqin Tian[9] builds time window according to the user log and evaluate the reliability of user in these time window. Lijie Fan[10] proposed a recommendation trust evaluation model based on rating in mobile e-commerce environment. Shao Zhang[11] builds a trust model for both users and merchants to ensure that they can trust each other. But there is still no research working on building an evaluation method to normal transaction.

3 TRANSACTION RISK FILTER MODEL

The purpose of the proposed transaction risk filter model is to pass as much as possible normal transactions before stringent model, so the primary problem is how to measure a transaction is normal. From the analysis of the distribution pattern of abnormal transactions by clustering method, we use distance discrimination between transaction and centroid of the main cluster of abnormal transactions for judging whether the transaction can be filtered. In this section, we will give the details of transaction risk filtering model. The data set we used in this paper is given in 3.1. 3.2 gives the analysis and selection of features, and talks about the feature weighted issue. 3.3 gives an analysis on abnormal transactions by DBSCAN cluster method and 3.4 gives the specific of transaction risk filtering model and details of distance discrimination process.

3.1 *Data sets*

The data sets of this paper are online credit card payment transaction logs provided by an electronic payment company in China. The transaction samples are produced between February and March in 2014. Due to the large amount of data, in this paper we randomly pick up about 2000 million transaction logs which contain about 4700 abnormal transaction, so the ratio of imbalanced sample is close to 0.02%. We will use the transaction logs in February as training data and logs in March as validation data in experiments. The original transactions log data items in this study are shown in Table 1.

Table 1 Transaction Log Data Item Details

Variable	Type	Definition
trans_no	char	transaction number
client_id	long	user client id
mac	char	mac address of the transaction platform
ip_addr	char	ip address of the transaction platform
trans_date	char	transaction time
trans_amount	double	transaction amount
card_index	long	hash value of card number
card_country	long	country of card
shipto_adr	char	shipping address
merchant_type	char	merchant type
case_flag	int	class type of transaction

3.2 *Feature Selection and Feature Weighted*

Let transaction class be Y, where Y has only two types which are normal and abnormal. We first need to extract features from transaction logs which is represented by X. Based on research of fraud detection feature on credit card[12], we extract and derive 40 features. We also select feature by applying IV(Information Value). IV is a very effective feature selection method with a wide range of application[13]. To applying IV first need to calculate WOE(Weight of Evidence) of each feature though transaction logs, which is calculated by formula(1). Where x_i is specific value of a feature, in this paper $x_i \in X_j$, and y_k stand for normal transaction class. WOE only can indicate the importance of specific value of feature to the target class, if we want to measure the importance of the entire feature, the introduction IV calculation will be necessary. IV can be calculated by formula(2).

$$Woe(x_i) = log\frac{f_{y=y_k|x=x_i}}{f_{y\neq y_k|x=x_i}} \quad (1)$$

$$IV(X_j) = \sum_{x_i \in X_j}\left(f_{y=y_k|x=x_i} - f_{y\neq y_k|x=x_i}\right)Woe(x_i) \quad (2)$$

Studies have shown that when IV above 0.1 indicates that the feature has a moderate degree of importance for classification, and if IV greater than 0.3 indicates that the feature has obvious effect for classification. This paper chose 0.1 as the criteria to select feature which will reduce the effects of noise feature. Table 2 is a table of partial screened features with their corresponding definition and IV. So we can construct transaction sample $e_i \in E$, $e_i=(x_1,x_2,...,x_n,y_k)$, where $x_i \in X_i$, $y_k \in Y$.

Table 2 features details after feature selection by IV

Variable	Definition	IV
X_1	the days from the earliest time the card had a transaction to now	1.41
X_2	square root of sum of transaction paid by this card in 15 days	1.06
X_3	the number of devices which have been used to pay with the card	1.02
X_4	total number of times of transaction paid by this card in 15 days	0.72
X_5	distance between billing address and login IP address	0.67
X_6	square root of sum of transaction paid by this card in 30 days	0.54
X_7	total number of times of transaction paid by this card in 30 days	0.49
X_8	total number of times of transaction happened in this hour that are paid by this card	0.33
X_9	total number of times that the transaction was set as this shipping address using this card	0.29
X_{10}	total number of times that this card was used to buy this merchant type	0.22
X_{11}	distance between shipping address and login IP address	0.21
X_{12}	total number of times that this card was used on this device	0.14
X_{13}	distance between shipping address and billing address	0.14

Because of the important differences between different features, we need to assign a certain weight to each feature. Previously, we have discussed the IV can reflect the importance of feature to discriminate between normal and abnormal transactions, thus we can calculate feature weight by their IV. Let the IV of feature X_i is v_i, then the weight w_i of feature X_i is calculated by the proportion of v_i in sum of all feature IV. w_i is calculated by formula(3).

$$w_i = v_i / \sum_{X_j \in E} v_j \quad (3)$$

3.3 *Analysis of Abnormal Transaction Based on DBSCAN cluster method*

In this paper, we have analyzed the distribution pattern of abnormal transaction samples by clustering. K-Means is commonly used as a simple and fast convergence clustering algorithm, but the number of cluster K should be specified before clustering and the selection of K will directly affect the quality of clustering results. Here, we can not specify how many cluster the abnormal transaction will gather, so we chose a clustering algorithm based on the spatial density called DBSCAN(Density-based Spatial Clustering of Applications with Noise) proposed by Ester Marthin[15]. DBSCAN algorithm does not need to specify the cluster amount and can detect noise data sample. DBSCAN requires that for each sample in one cluster, with a given radius *Eps*, the number of other samples in this cluster must bigger than a given threshold *MinPts*. So we need to specify *Eps* and *MinPts* for this clustering analysis.

We observe the distribution of abnormal transactions by applying DBSCAN clustering analysis on the transactions logs in February. We use both the original features and IV weighted feature to conduct the clustering experiment. We find that most abnormal transactions gather into one main cluster. Figure 2 show that when setting a radius of 86, abnormal transactions of main cluster account for 96.31%. Figure 2 also shows that the weighted feature will make the proportion of abnormal transactions of main cluster faster convergence and easier to exclude outliers.

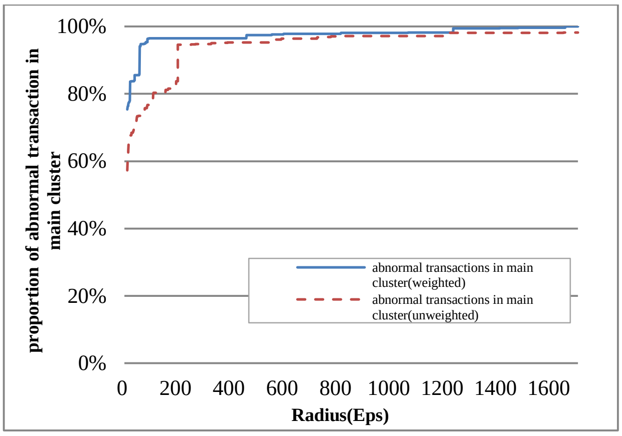

Figure 2 Relationship between the proportion of abnormal

transaction in main cluster and radius Eps

The result of clustering experiments shows that the abnormal transactions that is not in the main cluster account for a small proportion of the overall abnormal transactions, so here we consider these abnormal transactions as outliers. According to the statistical definition of small probability events, we will set a 0.05 threshold criteria and use an *Eps* which can make more than 95% abnormal transactions being in the main cluster. In this data set, when *Eps* is set to 86, the abnormal transactions in main cluster account for 96.31%, so we set *Eps* 86 as our further experiment parameter.

3.4 *Filter condition based on distance discrimination*

The purpose of this paper is to pass normal transactions, so the next issue is how to measure a transaction is normal. Here we define a normal transaction measure function $T(E)$ as a measure method to normal transactions and define the result of measure function is transaction reliability value. When the $T(E)$ is determined, we can use transaction reliability threshold to check if a transaction can be filtered.

Definition 1: Normal Transaction Measure Function $T(E)$ is a function mapping from feature vectors E to transactions reliability value.

Definition 2: If a transaction E can be filtered, if and only if $T(E) \geq \theta$, where θ is the transaction reliability threshold.

Based on the analysis of DBSCAN clustering in 2.3, we get that most of abnormal transactions are in the main cluster. Therefore, we use the distance between the transaction sample and centroid of abnormal transaction as the measure method of the difference between normal and abnormal transaction, i.e. transaction reliability value.

Let the centroid be $E^T=(X_1^T,X_2^T,...,X_n^T)$, we can get the centroid by calculate the center of main cluster after DBSCAN clustering. We use Euclidean distance as the measure function, so the $T(E)$ is calculated by formula(4). In the further experiment, we will get the center of the main cluster by the specific *Eps* which is selected by the criteria described in 3.3. We will also apply weighted feature to the calculation of $T(E)$, which is shown by formula(5).

$$T(E)=\sqrt{\sum_{X_i\in E}\left(X_i-X_i^T\right)^2} \qquad (4)$$

$$T(E)=\sqrt{\sum_{X_i\in E}\left(w_iX_i-w_iX_i^T\right)^2} \qquad (5)$$

Application of transaction filter model based on distance discrimination method is divided into offline training phase and online validation phase. Offline training phase will calculate the feature vectors of all transactions for offline training data and calculate the corresponding transaction reliability value. In the training phase we will select a transaction reliability threshold as the criteria to filter transaction in the online phase. And in online validation phase, we will calculate the transaction reliability value of online transaction using the center calculated in training phase and filter normal transaction based on the threshold.

So the selection of transaction reliability threshold determines the performance of the transaction risk filter model. In order to evaluate the performance of our filtering model, we will introduce two evaluation methods for this model which are pass rate and leak rate.

Definition 3: Pass Rate, indicating the proportion of normal transaction of the transaction that filtered by models in total normal transaction.

Pass rate can be calculated by formula(6).

$$E_1=\frac{TP}{TP+FN} \qquad (6)$$

Definition 4: Leak Rate, indicating the proportion of abnormal transaction of the transaction that filtered by models in total abnormal transaction.

Leak rate can be calculated by formula(7).

$$E_2=\frac{FP}{TN+FP} \qquad (7)$$

Where *TP*(True Positive) shows the number of the positive samples which is correctly classified as positive samples, *FP*(False Positive) shows the number of the negative samples which is incorrectly classified as positive samples, *TN*(True Negative) shows the number of negative samples which is correctly classified as negative samples and *FN*(False Negative) shows the number of positive samples which is incorrectly classified as negative samples.

For the risk filtering model we expect higher pass rate and lower leak rate at same time. Obviously, when the threshold is set to 0, the pass rate and leak rate will all be 100%. With the increase of threshold, both two evaluation value will decrease. Therefore, in training phase we should select the threshold based on the balance between pass rate and leak rate. In industry environment, we can get the threshold by determining leak rate depending on the business requirement.

4 EXPERIMENTAL RESULTS AND DISCUSSION

According to the formula (1) to (5), we calculate the transactions reliability value of transaction sample in February using weighted and unweighted Euclidean distance, and calculate both pass rate and leak rate depending on different transactions reliability threshold. The experimental results are shown in figure 3 and 4, where the abscissa stands for threshold. From figure 3 and 4, we can get that when the threshold increase, both pass rate and leak rate decrease, but the decrease speed of leak rate is faster than pass rate, indicating that this risk filtering model is more inclined to excluding normal transactions. From figure 3 and 4, we can also get that when using weighted feature the decrease speed of leak rate is higher than using original feature, which means that given a same leak rate, the weighted Euclidean distance can achieve a higher pass rate.

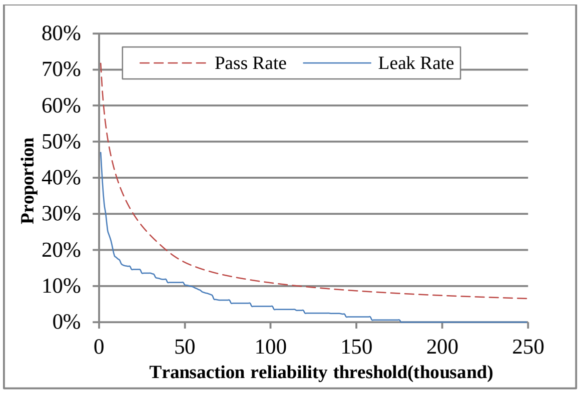

Figure 3 Pass rate and leak rate of ordinary Euclidean distance in February data set

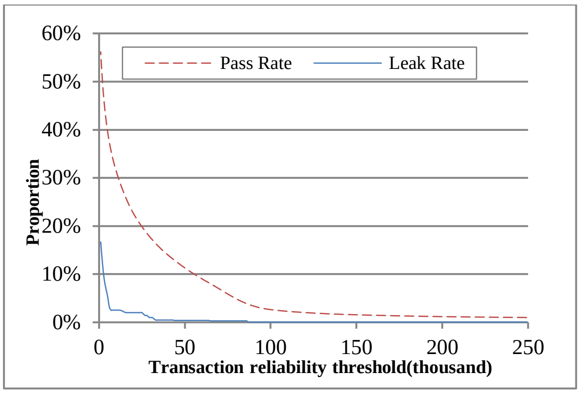

Figure 4 Pass rate and leak rate of weighted Euclidean distance in February data set

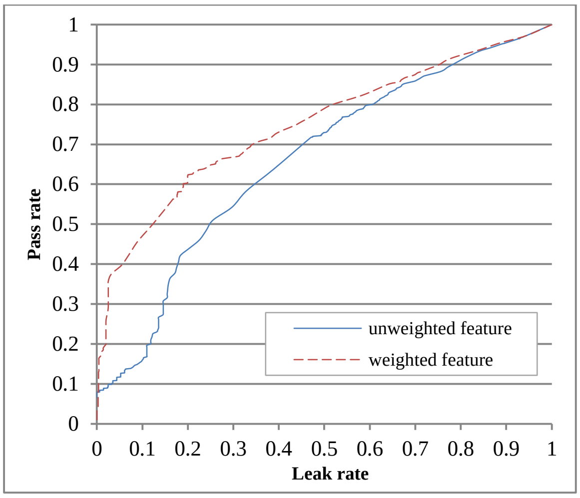

Figure 5 ROC curve of original and weighted Euclidean distance in February data set

This conclusion can be more clearly seen in the ROC curve. We also plot the ROC curve in Figure 5, where the abscissa is leak rate and the ordinate is the corresponding pass rate. Figure 5 shows that when using weighted Euclidean distance, the increase speed of pass rate is very high when the leak rate is below 5%, and finally grow to 39.69%, while at same time the pass rate of Euclidean distance using original feature is only 11.73%. And the ROC area of weighted Euclidean distance is obviously larger than unweighted Euclidean distance. Therefore, the weighted Euclidean distance method has a significant effect on improving the performance of normal transactions filtering.

The selection of transaction reliability threshold is mainly based on the specific requirements of the application scenarios, but we can also get some hints from ROC curves, i.e. select the highest possible efficiency threshold with a given pass rate or leak rate. According to figure 5, we select the point with most obvious slop change as threshold θ’ with leak rate 3.10% and pass rate 37.50%.

In order to verify that threshold will also have an effect on future transactions, we calculate the transaction reliability value of transactions samples in March using weighted Euclidean distance and analyze the pass rate and leak rate on difference threshold. The experimental result is shown in Figure 6. When the threshold is set to θ’, the results show that 39.20% normal transactions are filtered and only 0.68% abnormal transactions are incorrectly filtered.

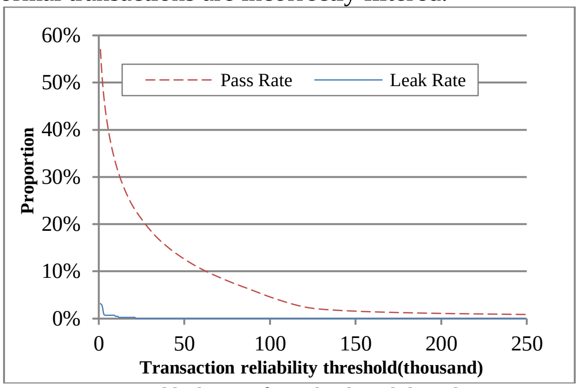

Figure 4 Pass rate and leak rate of weighted Euclidean distance in March data set

Experimental results show that transaction risk filtering model based on weighted Euclidean distance discrimination method has a significant effect on filtering the normal transactions. With a given leak rate, the model can achieve a high filtering effect. Using weighted feature based on IV has an improvement on filtering effect comparing to the original feature. Finally, the transaction reliability threshold analyzed in training phase has also a good filtering effect in validation phase, which means that the threshold calculated in offline data will also has an effect on filtering future online data.

5 CONCLUSION

This paper proposes a transaction risk filtering model to filter normal transaction before stringent model validation. Through this model, the e-payment company can reduce the burden and risk of additional strict model validation, reduce interference to normal users. The transaction risk filtering model can be integrated into the existing risk control system. This paper presents a method to filter normal transaction based on weighted Euclidean distance discrimination and apply the method and model in real transactions data set. The experimental results show that the model can achieve a great effect on filtering normal transaction while keeping a low leak rate.

The features and model we used in this paper has a good effect on filtering normal transactions, but the lack of theoretical and statistical analysis will reduce the universality of the features and model, so we will work on the analysis on the feature and method in future to increase the universality of them. In addition, the selection of threshold we used now is mostly based on experience and application requirements, we need to find a more scientific method to choose a suitable threshold. We will also do further research on normal transaction measure function to find a function which can achieve a better effect on normal transactions filtering.

ACKNOWLEDGMENT

This work is supported in part by the National Natural Science Foundation of China under Grant No. 61173014 and 61173016, Hong Kong, Macao and Taiwan Science & Technology Cooperation Program of China under Grant No. 2013DFM10100, Shanghai Science & Technology Research Plan under Grant No. 11JC1412800.

REFERENCES:

[1] Sherman E. Fighting web fraud[J]. Newsweek, 2002, 10.

[2] Phua C, Lee V, Smith K, et al. A comprehensive survey of data mining-based fraud detection research[J]. arXiv preprint arXiv:1009.6119, 2010.

[3] Phua C, Alahakoon D, Lee V. Minority report in fraud detection: classification of skewed data[J]. ACM SIGKDD Explorations Newsletter, 2004, 6(1): 50-59.

[4] KolaliKhormuji M, Bazrafkan M, Sharifian M, et al. Credit Card Fraud Detection with a Cascade Artificial Neural Network and Imperialist Competitive Algorithm[J]. International Journal of Computer Applications, 2014, 96(25): 1-9.

[5] Chen F H, Chi D J, Zhu J Y. Application of Random Forest, Rough Set Theory, Decision Tree and Neural Network to Detect Financial Statement Fraud–Taking Corporate Governance into Consideration[M]//Intelligent Computing Theory. Springer International Publishing, 2014: 221-234.

[6] Shen A, Tong R, Deng Y. Application of classification models on credit card fraud detection[C]//Service Systems and Service Management, 2007 International Conference on. IEEE, 2007: 1-4.

[7] Kumari N, Kannan S, Muthukumaravel A. Credit Card Fraud Detection Using Hidden Markov Model-A Survey[J]. Middle-East Journal of Scientific Research, 2014, 19(6): 821-825.

[8] Halvaiee N S, Akbari M K. A novel model for credit card fraud detection using Artificial Immune Systems[J]. Applied Soft Computing, 2014, 24: 40-49.

[9] Tian Li-Qin, Lin Chuang. Evaluation mechanism for user behavior trust based on DSW[J]. Journal of Tsinghua University(Science and Technology), 2010(5):763-767.

[10] Fan Li-jie, Wang Su-Zhen, Liu Wei, Evaluation method based on human trust mechanism for mobile e-commerce trust[J]. Computer Science. 2012, 39(1):190-192.

[11] Zhang S, Lu X, Wang B. A trust evaluation model behaviors based in electricity market[C]//Electric Utility Deregulation and Restructuring and Power Technologies, 2008. DRPT 2008. Third International Conference on. IEEE, 2008: 561-566.

[12] Wu Ting. Research on the applications of data mining in credit card fraud detection[D]. Southeast University, 2006.

[13] Wang Y, Wong A K C. From association to classification: Inference using weight of evidence[J]. Knowledge and Data Engineering, IEEE Transactions on, 2003, 15(3): 764-767

[14] Moez H, Alec Y C, Ray F. Variable selection in the credit cardindustry[A]. NESUG, 2006.61 -65

[15] Ester M, Kriegel H P, Sander J, et al. A density-based algorithm for discovering clusters in large spatial databases with noise[C]//Kdd. 1996, 96: 226-231.