# Research on transaction security detection algorithm for Large-scale e-commerce website

Hu Guixiang, Qian Xinjie, Fu Qiulin, Yang Bo

Yibin Vocational And Technical College, Yibin Sichuan, 644003

Keywords: e-commerce; security; transaction;

**Abstract:** The large-scale e-commerce website transaction security detection methods are studied. For the defect that the large-scale e-commerce website transaction security detection is susceptible to be interfered by ambient noise, a large-scale e-commerce website transaction security detection method based on characteristic attribute mapping model is proposed. According to principal component analysis method to process redundant transaction data of large e-commerce websites, so as to reduce the complexity of the data. Characteristic attributes mapping model is established to achieve intrusion detection when transacting on the large-scale e-commerce website, to determine the security of transactions. Experimental results show that the use of proposed algorithm for large-scale e-commerce websites transaction security detection, can greatly improve the accuracy of detection, so that obtaining satisfactory results.

## 1 Introduction

With the continuous development and popularity of large-scale e-commerce technology, large-scale e-commerce websites transaction security has been paid more and more attention [1]. Therefore, the large e-commerce websites transaction security detection technology has become a core issue to be studied in the field of e-commerce, has collected widespread concern of many experts and scholars [2]. In the large e-commerce website security detection process, how to detect the illegal data in large-scale e-commerce transactions, has become a major topic on the aspect of transaction security detection [3]. At this stage, the major large-scale e-commerce websites transaction security detection methods include the transactions security detection method based on K-means clustering algorithm, the transactions security detection method based on ant colony algorithm and the transactions security detection method based on support vector machine algorithm [4-6]. Among them, the most commonly used detection method is based on support vector machine algorithm. Due to a very bright future of large e-commerce websites transaction security detection method, it subject to the attention of many experts, and become the focus of the problem being studied.

## 2 The optimization principle of large e-commerce websites transaction security detection method

### *2.1 Principal Component Analysis*

In the process of large-scale e-commerce website transactions, all transaction data are necessary to constitute a collection $\{z_1, z_2, \cdots, z_p\}$. The initial threshold of principal component analysis for a large e-commerce website transactions data can be described by $b_k$, the following equation can be adopted to simplify the large e-commerce websites transaction data:

$$\begin{cases} H_1 = c_{11}b_1 + c_{12}b_2 + \cdots c_{1p}b_p \\ H_2 = c_{21}b_1 + c_{22}b_2 + \cdots c_{2p}b_p \\ \cdots \\ H_p = c_{p1}b_1 + c_{p2}b_2 + \cdots + c_{pp}b_p \end{cases} \quad (1)$$

In the above formula, the correlation between $H_k$ and $H_l$ is poor, and there is no mutual restriction, $H_k$ can be used to describe the main component of transaction data, the following equation can be utilized to describe the matrix consisted of the ratio of transaction data:

 

$$D = \begin{bmatrix} c_{11} \cdots c_{12} \cdots c_{1p} \\ c_{21} \cdots c_{22} \cdots c_{2p} \\ \cdots \\ c_{p1} \cdots c_{p2} \cdots c_{pp} \end{bmatrix} \quad (2)$$

With principal component analysis method to analyze large e-commerce websites transaction data, the process is as follows:

(1) In the process of large-scale e-commerce website transactions, the acquired transaction data is initialized to provide the basis for transaction security detection.

(2) By calculating to obtain the operation characteristics of a large e-commerce websites transaction security is threatened, and calculate the ratio of the above characteristics.

(3) According to the operation characteristics when a large e-commerce websites transaction security is threatened to calculate, so as to obtain corresponding feature vectors.

(4) According to the operation characteristics when a large e-commerce websites transaction security is threatened to classify, so as to acquire the main components in the transaction security detection process.

(5) Based on the main component of transactions security detection, it is possible to calculate the amount of corresponding data.

According to the method outlined above, it is possible to simplify the transactions by removing the redundant data in transaction process and reduce the complexity of detection, so that providing the basis for transaction security detection.

*2.2 achievement of large-scale e-commerce websites transaction security detection*

The feature attribute mapping model is built to achieve large-scale e-commerce websites transaction security detection. Its details are as follows:

During the setting process of a large e-commerce websites transaction security detection, the data need to be inputted is $(a_1, b_1), (a_2, b_2), \cdots, (a_Q, b_Q)$, the range of value outputted from the transaction characteristics attribute mapping model is $b_l \in \{-1, 1\}$. $i(a)$ represent data classification function in the large e-commerce websites transaction security detection process. Assuming the output of characteristic attribute mapping model is $b_l = -1$, it is determined that the data belongs to secure transactions, assuming that the output of this model is $c_m = -1$, then it is determined that the data belongs to the data of transaction risk. The value of classification function can be calculated according to the following formula:

$$b = i(a) = z^T \eta(a) + e \quad (3)$$

Where, $\eta$ represents characteristic mapping relevance during the large e-commerce websites transaction security detection process, $z$ indicates the ratios of operating characteristic when the transaction security is threatened.

Based on the above transaction data to process E-commerce websites transaction security detection, transaction data classification results obtained are as follows:

$$\min_{z,e,h} M(z,h) = \frac{1}{2} z^T z + \frac{1}{2} \lambda \sum_{l=1}^{Q} h_l^2 \quad (4)$$

In the transaction data classification process, constraints for classification are as follows:

$$b_l [z^W \eta(a_l) + e] + h_l = 1 \quad (5)$$

By the method outlined above, the principal component analysis is capable to be utilized to process the redundant data in transaction operating behavior, thereby reducing the complexity of the transaction data. Characteristic attribute mapping model is established to achieve large-scale e-commerce websites transaction security detection.

## 3 Simulation results analysis

In order to evaluate the effectiveness of large-scale e-commerce websites transaction security detection method based on characteristic attribute mapping model, a single experiment is needed to be conducted. During the experiment, the experiment needs to be programmed with the JAVA language.

With traditional algorithms and proposed algorithm to conduct large-scale e-commerce websites transaction security detection, assuming the transaction have insecure operation, the system will be alarming, otherwise, it will be no alarming, the comparison of false alarm rate obtained by the experiment can be described by the following graph:

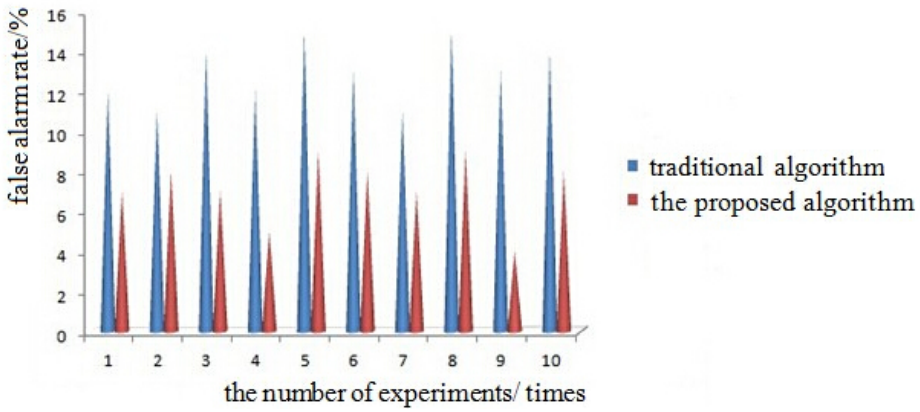


**Figure 1 comparison of false alarm rate in different algorithms**

The relevant data in the above experiments process were analyzed, Table 1 can be obtained as below:

**Table 1 Experimental data tables of different algorithms**

| The number of experiments | the traditional algorithm time (ms) | The traditional algorithms false alarm rate (%) | The proposed algorithm time (ms) | The proposed algorithms false alarm rate (%) |
|---|---|---|---|---|
| 1 | 45 | 12 | 23 | 7 |
| 2 | 48 | 11 | 27 | 8 |
| 3 | 44 | 14 | 22 | 7 |
| 4 | 47 | 12 | 28 | 5 |
| 5 | 44 | 15 | 25 | 9 |
| 6 | 43 | 13 | 22 | 8 |
| 7 | 48 | 11 | 27 | 7 |
| 8 | 42 | 15 | 28 | 9 |
| 9 | 48 | 13 | 25 | 4 |
| 10 | 45 | 14 | 28 | 8 |

According to the experimental data can be known, with the proposed algorithm to perform large-scale e-commerce websites transaction security detection, detection time is shorter than the traditional algorithm, the false alarm rate is lower than traditional algorithm, which demonstrating the superiority of the algorithm.

## 4 Conclusion

This paper presents a large-scale e-commerce webwebsite transaction security detection method based on characteristic attribute mapping model. According to principal component analysis method to process redundant transaction data of large e-commerce websites, so as to reduce the complexity of the data. Characteristic attributes mapping model is established to achieve intrusion detection when transacting on the large-scale e-commerce website, to determine the security of transactions. Experimental results show that the use of proposed algorithm for large-scale e-commerce websites transaction security detection, can greatly improve the accuracy of detection, so that obtaining satisfactory results.

## References

[1] Liu Tao, Pi Guoqiang. Application of Immune Algorithm in Network Intrusion Detection [J]. Computer simulation, 2011.11：91-94

[2] Dai Tianhong, Wang Keqi, Yang shaochun. Intrusion Detection Research Based on Support Vector Machine [J]. China safety science journal, 2008, 18(4):126-130.

[3] Wang Tao, Gong Huili. Application of Support Vector Machine in the Intrusion Detection System [J]. Control & management, 2006, 22(12):89-91.

[4] Zhang Qiuyu, Jie Yang, Li Kai. Method of membership determination for fuzzy support vector machine [J] Journal of Lanzhou University of technology, 2009, 35(4):89-93.

[5] Wang Xingdong, She Kun, Zhou Mingtian, Liu Heng. Intelligent IDS based on BP neural network [J]. Journal of Chengdu University of information technology, 2005, 20(1):1-4.

[6] Xiao Haijun, Hong Fan, Zhang Zhaoli, Liao Junguo. Intrusion Detection Based on a Fusion Classifier and SVM [J]. Computer simulation, 2008, 25(4):130-132.