Available online at www.sciencedirect.com
ScienceDirect
ELSEVIER
June 2016, 23(3): 29–36
www.sciencedirect.com/science/journal/10058885
The Journal of China Universities of Posts and Telecommunications
http://jcupt.bupt.edu.cn

User abnormal behavior analysis based on neural network clustering

Zheng Ruijuan[1], Chen Jing[1] (✉), Zhang Mingchuan[1], Zhu Junlong[2], Wu Qingtao[1]

1. College of Information Engineering, Henan University of Science and Technology, Luoyang 471000, China
2. State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China

Abstract

It is the premise of accessing and controlling cloud environment to establish the mutual trust relationship between users and clouds. How to identify the credible degree of the user identity and behavior becomes the core problem? This paper proposes a user abnormal behavior analysis method based on neural network clustering to resolve the problems of over-fitting and flooding the feature information, which exists in the process of traditional clustering analysis and calculating similarity. Firstly, singular value decomposition (SVD) is applied to reduce dimension and de-noise for massive data, where map-reduce parallel processing is used to accelerate the computation speed, and neural network model is used for softening points. Secondly, information entropy is added to hidden layer of neural network model to calculate the weight of each attribute. Finally, weight factor is used to calculate the similarity to make the cluster more accuracy. For the problem of analyzing the mobile cloud user behaviors, the experimental results show that the scheme has higher detection speed (DS) and clustering accuracy than traditional schemes. The proposed method is more suitable for the mobile cloud environment.

Keywords anomaly analysis, information security, singular value decomposition (SVD), neural network, information entropy

1 Introduction

With the rapid development of mobile cloud computing, the mobile cloud service [1] business is bound to explosive growth. Therefore, people begin to store all kinds of information from computers to the cloud to reduce the constraints of its limited resources such as storage and computing resources. It brings convenience to work and life for people while also makes information security face severe tests.

With all kinds of hackers and intrusion behaviors emerging in endlessly, network attack technology becomes more mature and changeable, and the traditional passive defense means cannot solve mobile cloud user information security issues significantly. Facing of various passive defensive measures, people are more inclined to proactive detection techniques such as analysis to the abnormal behavior [2].

Received date: 12-11-2015
Corresponding author: Chen Jing, E-mail: 15036775207@163.com
DOI: 10.1016/S1005-8885(16)60029-8

Anomaly analysis [3] was proposed by James Anderson, whose main idea is modeling by some statistics of user behaviors to discover the ‘invaders’. The premise of abnormal analysis is assuming there are big differences between normal and abnormal behavior. The normal data is used to build model which can process the identifying data. If the matching results exceed the setting threshold, it will be regarded as an abnormal behavior.

Analyzing user abnormal behavior is actually the clustering problem [4], where the behaviors are clustered in two classes, i.e. “normal” and “abnormal”. Behaviors in the same class or cluster have higher similarity, while those in different clusters have lower similarity. The fact of abnormal analysis is how to divide the behaviors into several classes or clusters.

This paper merges together the ideas of SVD, neural networks and information entropy, which avoids the traditional clustering analysis problems of sensitive to noise and over-fitting. It uses information entropy and weight of attribute to calculate weight factor and similarity respectively, which makes the cluster more accuracy.

Based on the inherent defects of mobile terminals, this paper focuses on the abnormal behavior analysis method from user trusting aspect. The user requests will be received by wisdom mapping layer for further processing only when the user behavior is normal. Both analysis and simulation results indicate that our scheme outperforms other similar schemes.

2 Related works

Calculating similarity is very important to analyze user abnormal behavior. Several references in the field of user abnormal analysis have been summarized. The most common method is calculating the distance between sample properties. Ref. [5] used Euclidean distance to measure the similarity of attributes, which not only could measure the two-dimensional linear space, but also *d*-dimensional linear space. Ref. [6] used the lexical similarity *k*-means algorithm based on fuzzy logic Euclidean distance. It could improve the accuracy of the similarity estimation. Ref. [7] improved the *k*-means clustering algorithm performance, which uses the window technology in the process of clustering. Ref. [8] introduced segmental *k*-means algorithm into hidden semi-Markov model (HSMM) to train algorithm, where used the average information entropy of fixed-length observed sequence as the anomaly detection metric. These methods have two flaws. First, it cannot detect flood attacks. Second, it supposes that the weight of each attribute is equal, which floods the real weight of each attribute and greatly reduces the clustering accuracy.

The traditional clustering analysis is a hardening of the points, the classification category boundaries are distinct, which is likely to cause over-fitting. In fact, most of the objects have no strict attribute boundaries and suitable for softening points. Ref. [9] proposed the Bias-correction fuzzy clustering algorithms to avoid the hard clustering. It overcomes the poor clustering results and poor initializations. Refs. [10–11] calculated the information entropy of all records in the training dataset and the weight of each attribute with information entropy, which avoids the average and human interference to weight of each attribute and improves the clustering accuracy.

In order to make the analysis results more accuracy, Refs. [12–13] introduced neural network into the process of clustering, using the inherent attributes of self-learning, self-adaptive, associative memory and association mapping to increase the detection of ambiguity. Ref. [14] proposed a new anomaly detection algorithm, which used improved hierarchy clustering to overcome the problems of high noise and data updated. Liu et al. [15] researched user behavior of mobile terminal to mine the correlation between user pressure and user unsafe behavior to prevent the malicious and unsafe behavior of users.

In short, there are some useful researches lay solid foundations for the user dependability. It is quite important for communicating between mobile cloud and its users to complete the process of series operations in the mobile cloud environment future. Nevertheless, most researches on clustering focus on the user behaviors or softening points by the neural network model. Those researches ignore the different intrinsic property of object, while it is different in practice. The existing literatures have not yet the concrete method to calculate standardized weights and soften points completely.

3 System models

3.1 SVD model

SVD model [16] is earliest and most widely used in image processing field to reduce the time complexity and improve the efficiency during feature extraction. It has better scalability and practicality, and it is easy to integrate with other technologies to improve the performance. SVD model is as follows:

$$\begin{pmatrix} X_{11} & X_{12} & X_{13} & \cdots & X_{1m} \\ X_{21} & X_{22} & X_{23} & \cdots & X_{2m} \\ \vdots & \vdots & \vdots & & \vdots \\ X_{n1} & X_{n2} & X_{n3} & \cdots & X_{nm} \end{pmatrix}$$

For any real matrix $\boldsymbol{A}$ with $n \times m$, there always are m orders orthogonal matrix $\boldsymbol{U}$ and n orders orthogonal matrix V, which makes $\boldsymbol{A}=\boldsymbol{U}\boldsymbol{\Delta}\boldsymbol{V}^{\mathrm{T}}$, where $\boldsymbol{\Delta}=\operatorname{diag}(\delta_1,\delta_2,\ldots,\delta_r)$, $\delta_i>0(i=1,2,\ldots,r), r=\operatorname{rank}\boldsymbol{A}$, the singular values of matrix $\boldsymbol{A}\boldsymbol{A}^{\mathrm{T}}$ and $\boldsymbol{A}^{\mathrm{T}}\boldsymbol{A}$ are $\lambda_1 \geqslant \lambda_2 \geqslant \ldots \geqslant \lambda_r > 0$, $\lambda_{r+1} = \lambda_{r+2} = \lambda_m = 0$, we call positive number $\delta_i = \sqrt{\lambda_i}(i=1,2,\ldots,r)$ are singular value of matrix $\boldsymbol{A}$. If setting $\boldsymbol{U}=(u_1,u_2,\ldots,u_m)$, $\boldsymbol{V}=(v_1,v_2,\ldots,v_m)$, then u_i and $v_i(i=1,2,\ldots,r)$ are the eigenvectors corresponding with λ_i^2 of $\boldsymbol{A}\boldsymbol{A}^{\mathrm{T}}$ and $\boldsymbol{A}^{\mathrm{T}}\boldsymbol{A}$ respectively, and it introduces vector u_i and v_i is to make $\boldsymbol{U}$ and $\boldsymbol{V}$ form orthogonal matrix.

3.2 SVD de-noise model

For each information sub-matrix $X(N)=\{x_1,x_2,\ldots,$