Journal of Electronic Research and Application
OPEN

BIO-BYWORD
SCIENTIFIC PUBLISHING PTY LTD

Research on Reduced Optimization of Illegal Access Information in Database Internal and External Network

Zhou Cheng, Zhang Bo, Li Qian Mu

Abstract: The research on the optimization of the illegal access to the database inside and outside the network can effectively improve the security of the network database. Accurate reduction of illegal access to information, the need for accurate collection of known data, and its repeated nuclear iteration, so that the known access to a linear distribution of data to complete the information to restore. The traditional method of data mining into the access to the data filtering process, but the processing of information data linearity difference, resulting in the reduction effect is not good. Proposed multi-core composite internal and external network illegal access to information collection and accurate reduction method. Set the illegal information collection interval to calculate the address of the database illegal access to information, the use of SSL encryption mechanism to encrypt the information collected, the same type of illegal access to information in the known data for repeated nuclear iteration, to promote similar illegal The access information is linearly distributed in the super - high - dimensional Euclidean space, and the regression equation is integrated into the KRR to complete the illegal access information acquisition and accurate reduction. The simulation results show that the proposed method has strong robustness and can improve the security of the internal and external network information.

Key words: Database internal and external network; illegal access; information reduction

1 Introduction

In the country, with the rapid development of information and communication and network technology, the database has become the majority of institutional organizations, enterprise business information storage platform [1-3]. However, the frequent intrusion of data inside and outside the network at the same time, because most of the network database has a wide coverage, high value of information, storage data, the advantages of large, so the user's illegal intrusion of the database will be information in the database Security has a huge impact, in this case, the full protection of legitimate users of the legitimate access to the database, reduce the database from illegal access and modify the probability of becoming a database area to solve the major problems [4-6]. And the illegal access to the database inside and outside the network of illegal access to information collection and accurate reduction method can be integrated into the KRR method to set up unknown information regression equation, thus completing the database internal and external network illegal access to information collection and accurate reduction is an effective means to solve these problems, causing a lot of experts and scholars attention, but also a lot of good results [7].

[8] proposed a dynamic network based on the database inside and outside the network of illegal access to the information collection and accurate reduction method. The method firstly illegally accesses the information according to the history of the database, periodically carries out data mining on the illegal access information, and generates the rules, and introduces the rule into the audit diary filtering of the collection, which is integrated into the difference distribution method to complete the database internal and external network Illegal access to information collection and accurate reduction methods. The method is simpler, but there is a problem that the method is more restrictive. [9] proposed a CDTD database based on illegal access to the information collection and accurate reduction method. This method first gives the connection metering system database and the local data collection database, removes the illegal access information that has been transmitted, transmits all the illegal access information that is not transmitted, and returns the collected illegal access information into the function code position of the decimal in-

(Global Energy Internet Research Institute, Nanjing 210003)

formation word , Thus completing the database illegal access to information collection. The method is robust, but when the information is collected and restored by the current method, the loss of unknown illegal access information is large, and there is a problem that the illegal access information is reduced. In [10], we focus on the method of database access and information retrieval based on application layer protocol. This method introduces the TCP protocol into the database internal and external network illegal access information collection and restoration process, the protocol type as the information acquisition flag processing, integration of the call string matching method to complete the database illegal access to the information collection and accurate reduction. The method of information reduction is more efficient, but there is a problem of poor robustness of the method.

Aiming at the above problems, this paper proposes a method of database access and precision reduction based on multi -core compound database. The simulation results show that the proposed method has strong robustness and can improve the security stability of the database system.

2 Database internal and external network illegal access to information collection and accurate reduction principle

In the database of internal and external network illegal access to information collection and accurate reduction process, give the information collection time interval, the current collection of illegal access to information into the dynamic data group, the characteristics of different types of information, on the basis of The data is encrypted and transmitted, the regularity and relevance of the information are given, and the different local information is merged to complete the information acquisition and accurate reduction of the database. The specific steps are as follows:

Assuming that μ represents the user access behavior type, ∂ represents the amount of data transferred over a period of time in the database communication port, and $\wp(a)$ represents the main characteristic of the user's access behavior, the time interval for information collection is

$$\eta(E)=\frac{\mu\otimes\wp(a)}{\partial\otimes\Phi}\times\mathrm{H}(Z) \tag{1}$$

Where Φ represents the user's normal behavior pattern and H(Z) represents the user behavior data.

Suppose that $\theta(a)$ represents the audit data to select the user action behavior information, $\xi(j)$ represents the external audit data source import interface, $\varpi(z)$ represents that the message arrives before the message arrives at the destination window, the currently acquired illegal access information is input to the dynamic data group, statistics of different types of information are characterized by

$$q^{*}(C)=\frac{\varpi(z)\otimes\xi(j)}{\theta(a)}\otimes\frac{\Upsilon(a)\times\varsigma(f)}{\mu(W)}\times\varepsilon \tag{2}$$

Where $\Upsilon(a)$ represents the frequent event type in the security audit, $\varsigma(f)$ represents the system image partition, $\mu(W)$ represents the flag of the application protocol, and ε represents the number of audit analysis modules.

Assuming that $\gamma(z)$ represents the network to send the event notification message, $\varpi(g)$ represents the coordination task progress, $\hbar(x,v)$ represents the storage location of the original data, and $\varsigma(j,i)$ represents the acquisition interval time calculation module, the encrypted data is encrypted and transmitted as

$$\sum_{j-1}A(\upsilon)=\frac{\gamma(z)\otimes\varpi(g)}{\varsigma(j,i)}\odot\Phi(a)*\hbar(x,v) \tag{3}$$

Where $\Phi(a)$ is the number of changes in the number of information records.

Assuming that ν''' is the change of the number of information records represented by the collection points, the different local information is fused to give the regularity and relevance of the information

$$W'''(S)=\frac{\nu'''\times\sum_{j-1}A(\upsilon)\otimes\Phi}{q^{*}(C)}\otimes\Gamma(i) \tag{4}$$

Assuming that $\Re[d]$ represents the size of the restored data, $\lambda^{s}(q)$ represents the statistical count of the characters, then the database is illegally accessed by the information collection and accurate reduction

$$\bigcirc(b)=\frac{\lambda^{s}(q)\times\Re[d]}{W'''(S)} \tag{5}$$

In summary, it can be said that the database illegally access information collection and accurate reduction principle, the use of the principle of the database to complete the illegal access to internal and external network information collection and accurate reduction.

3. Data Collection and Restoration Method for Illegal Access to Database Based on Multi - core

Compound

3.1 Illegal access to information collection

In the database, illegal access to information collection and accurate reduction process, first set the database illegal access to information collection and acquisition interval to calculate the address of the database illegal access to information, the use of SSL encryption mechanism for encrypted information transmission. The specific steps are as follows:

Assuming that $E(v_1, v_2, \ldots v_3)$ is the collection of illegal access information collected from the information server represents an integer, ∂_w represents a combination of recent access data stream information, satisfies the condition $s = 1, 2, 3 \ldots n$, $\mu(s)$ represents each information entry, and each $\mu(s_n)$ describes the characteristics of the data stream information , then set the database to obtain illegal access to information collection and acquisition interval

$$Q^{*}(e) = \frac{\mu(s_n) \otimes E(v_1, v_2, \ldots v_3)}{\mu(s) \otimes \mathrm{N}^{(g)} \times \partial_w} \otimes \Re^{*}(a) \tag{6}$$

Where, $\mathrm{N}^{(g)}$ is a certain period of time the main changes in user behavior characteristics, $\Re^{*}(a)$ is the input buffer size.

Assuming that $\Phi(s)$ is the time of collecting information data by one time, $\mathrm{K}^{(x)}$ represents the set of connection strings and $\hbar(q)$ is the source values corresponding to each information word, the collected information data can be preprocessed

$$\eta(E) = \frac{\hbar(q) \times \Phi(s)}{\mathrm{K}^{(x)} \otimes \mathrm{N}(A)} \times \mu(Z) \otimes \mathrm{I}(F) \tag{7}$$

Where, $\mathrm{N}(A)$ is the number of information collection points, $\mu(Z)$ representing the collection of various collection points, $\mathrm{I}(F)$ representing the acquisition of information on the conversion process.

It is assumed that ∂^{x} is the collected data is stored in a temporary location by storing is the data stored in the temporary table, $\nu(k)^{*}$ representing the local network access data stream $\Im(S)$ representing the original information data stored in the form of a file, and storing the collected information by periodic storage

$$\eta^{s}(q,m) = \frac{\Im(S) \otimes \nu(k)^{*}}{\partial^{x}} \otimes \frac{R(Z) \oplus \mu(\varpi)}{\vartheta} \times \iota(C) \tag{8}$$

In this case, $R(Z)$ represents the communication security channel established by the local and the information server, $\mu(\varpi)$ represents the trust value of the data cache entry stored in the temporary table, ϑ^{*} represents the redundancy of the information, and $\iota(C)$ represents the audit flow of the access message.

Assuming that $\varpi(Z)$ is the position of the function code representing the information word $\mathrm{B}(it)$ represents the position of the synchronization word and the information word in the character string, the address of the database illegal access information is calculated

$$\mathrm{P}^{*}(\mathrm{H}) = \frac{\mathrm{B}(it) \times \varpi(Z)}{\theta(x) \times \Upsilon(e)} \otimes c(\varphi) \times \Phi(x) \tag{9}$$

Where $\theta(x)$ represents the array *bD* dimension, $c(\varphi)$ represents the periodic generation rule table, $\Upsilon(e)$ represents the number of similar visits, and $\Phi(x)$ represents the information of the latest time interval extracted at regular intervals.

Assuming that $\lambda(z)$ represents the information audit server, ψ represents the information management interface, the SSL encryption mechanism is used to encrypt the collected information to

$$\iota'''(R) = \frac{\psi \times R(Z)}{\lambda(z)} \mp \frac{\eta^{S}(q,m)}{\ell_{\varrho}^{*}(s,g)} \mp \mu(d) \times \mathrm{H}_{\varpi}'' \tag{10}$$

Where, $\ell_{\varrho}^{*}(s,g)$ is the SSL notarization mechanism, $\mu(d)$ is the information collection and information server communication between the use of TCP protocol, H_{ϖ}'' representing the authenticity of the information threshold.

In summary, it can be explained that in the database of internal and external network illegal access to information collection and accurate reduction process, the first set of illegal access to information collection and acquisition interval to calculate the address of the information, the use of SSL encryption mechanism for encrypted information transmission, Which lays the foundation for realizing the information acquisition and precision reduction of the illegal access to the database.

3.2 Reduction of Illegal Access Information of Internal and External Networks Based on Nucleation Iteration

Based on the illegal access information collected after the transmission in the 3.1 section, the iterative information of the same kind of information is carried out on the basis of the illegal access information and the exact process of the illegal access to the database. Restoring Illegal Access to Database Behavior. The specific steps are as follows:

Suppose that σ represents the kernel parameter of the Gaussian kernel function, x represents $x_1, x_2, \dots, x_n$ isomorphic unknown data, $x_1, x_2, \dots, x_n$ represents the same known data point of the low-dimensional Euclidean space, and in section 3.1 obtains the $\iota^m(R)$ access to information, the use of (11) on the same type of illegal access to information in the known data for repeated nuclear iteration, so that the known illegal access to information in the ultra-high dimensional Euclidean space linear distribution of state

$$\varphi_{n+1}(x) = \frac{\iota^m(R) \otimes \sigma}{(x_1, x_2, \dots, x_n) \otimes \omega} \times s[x_i, x_j] \times \varphi(x_i) \times \varphi(x_j) \quad (11)$$

Where *s* represents a *N*-dimensional space containing *M* points, x_i and x_j represent any two points in space, $\varphi(x_i)$ and $\varphi(x_j)$ represent the nucleation points of x_i and x_j

It is assumed that when the information data is linearly distributed in the super-high dimension Euclidean space, w represents the unit direction vector of the data of the hypervariable Euclidean spatial information data, the regression equation fused to the KRR method to form unknown information is

$$\mathrm{P}_{*}^{*}(\delta) = \frac{\varphi_{n+1}(x_i) \otimes \gamma(\aleph)}{\lambda_{(\varsigma)} \otimes I(R)} \times \iota(E) \quad (12)$$

Where $\gamma(\aleph)$ represents the port number, $\lambda_{(\varsigma)}$ represents the kernel parameter of the polynomial kernel function, $I(R)$ represents the determined regularization parameter, and $\iota(E)$ represents the linear space of the transformed data point regression.

From the calculation of the formula (12) can be analyzed, the known information data points closer to the linear, the more stable the data closer to the real, then use the formula (13) to complete the restoration of illegal access to information

$$\mathrm{X}_{\circ}^{*} \cdot (\kappa)^{\tau} = \frac{\mathrm{P}_{*}^{*}(\delta) \times \iota(E)}{\varphi_{n+1}(x_i)} / f(x) \quad (13)$$

Where $f(x)$ represents the regression function.

4 Proof of simulation

In order to prove that the proposed multi-core composite information database based on the internal and external network of illegal access to information collection and accurate reduction of the true effectiveness of the need for an experiment. Experiment in the CPU environment to build information database for illegal access to information collection and accurate reduction of the simulation platform. Experimental data from the MY SQL database, XDAS through the 7629 port to receive Winpooch acquisition of behavioral information data.

4.1 Different methods of illegal access to information collection effectiveness.

Respectively, based on the multi-core composite method and traditional CDTD method for information database for illegal access to information collection and accurate reduction experiments. This paper compares the security and efficiency of two kinds of methods for illegally accessing the information acquisition, and uses the results of the comparison to measure the effectiveness of the different methods for the illegal access to the information database. The comparison results are shown in Fig. 1 and Fig.2.

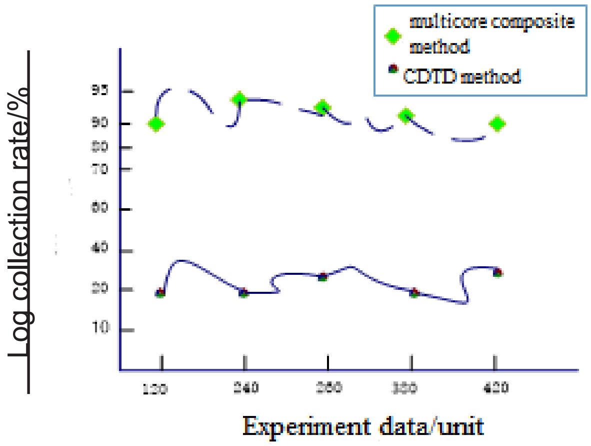

Figure 1 Comparison of the efficiency of different methods of information collection

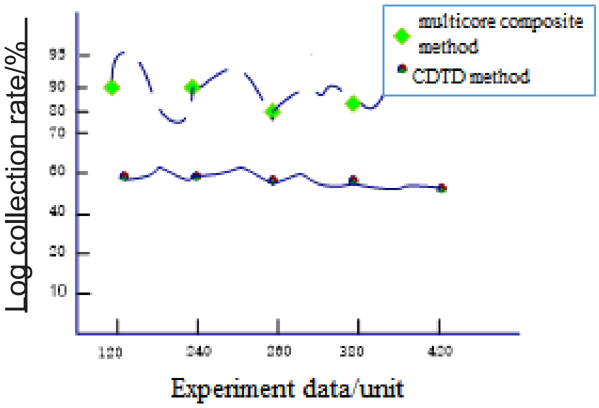

Figure 2 Different methods of information collection security comparison

It can be concluded from Fig. 1 and Fig. 2 that the validity of illegal access information acquisition based on multi-core compound method is better than that of CDTD method, which is mainly due to the use of In this paper, based on the multi-core composite method for illegal access to information collection, the first set the database to obtain illegal access to information collection and acquisition interval to calculate the address of the database illegal access to information, the use of SSL encryption mechanism for encrypted information transmission, thus ensuring the In this paper, the effectiveness of illegal access to information collection based on multi-core composite method is proposed.

4.2 The accuracy and stability of different methods for the reduction of illegal information

Based on the multi-core composite method and the traditional CDTD method, the information acquisition and precision reduction experiment of the internal and external network for information database is carried out respectively. Comparison of different methods to restore the accuracy and stability of information, the results shown in Figure 3 and Figure 4.

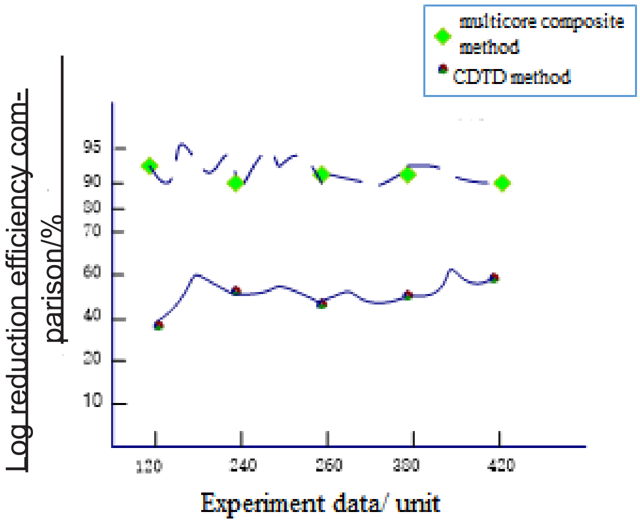

Figure 3 Comparison of different methods of information restore accuracy

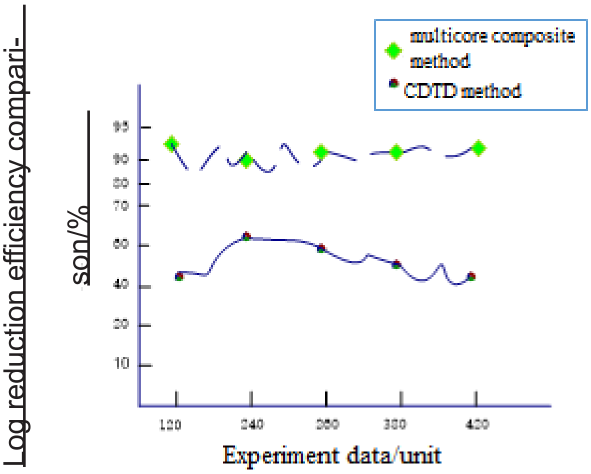

Figure 4 Comparison of different methods of information reduction efficiency

It can be analyzed from Fig. 3 and Fig. 4 that the accuracy and efficiency of the information reduction based on the multi-core composite method is better than that of CDTD method, which is mainly due to the use of this paper When the method is used to restore the information, the known data in the same kind of illegal access information is subjected to repeated iteration, and the known illegal access information is linearly distributed in the super-high dimension Euclidean space, and the known information pair Unknown data is linearly expressed and fused into the regression equation of the unknown information in the KRR method, which improves the accuracy and efficiency of the information reduction method proposed in this paper.

The simulation results show that the proposed method has strong robustness and can improve the security stability of the information database system.

5 Concluding remarks

In the case of information collection and restoration using the current method, the loss of unknown illegal access information is large, and there is a problem that the illegal access information is low. This paper proposes a method of collecting and verifying the illegal access information of database internal and external network based on multi-core compound. The simulation results show that the proposed method has strong robustness and can improve the security of the database information system.

References:

[1] Ding Lianghong. Big Dog Four-Legged Robot Key Technology Analysis [J]. Journal of Mechanical Engineering, 2015,51 (7): 1-23.

[2] GAO Jing, XUE Feng. Auditing of Enterprise Application System Based on Web Log [J]. Information Security & Technology, 2015,6 (6): 68-70.

[3] Jing Bo, Liu Ying, Chen Geng. Study on Database Log Analysis Method based on Petri Net [J]. Computer Science, 2014,41 (6): 250-253.

[4] Chen Yang. A New Generation Of Internet Log Audit System Based on Bypass Access [J]. Enterprise Technology Development: Academic Edition, 2015,34 (12): 36-38.

[5] YAO Yao, XIA Bin. Application of Phase Frequency Feature Group Delay Algorithm in Database Differential Access [J]. Computer Simulation, 2014,31 (12): 238-241.

[6] SUN Mei-wei. ADO.NET Database Access Technology based on C # Application [J]. Journal of Jilin Institute of Engineering Technology, 2014,30 (4): 85-87.

[7] Luo Can, et al. Application of Database Access Technology based on LabVIEW in Spindle Parameter Test [J]. Journal of Chinese Society of Agricultural Mechanization, 2014,35 (5): 261-263.

[8] Huang Baohua, Jia Fengwei, Wang Tianjing. Database Access Control Strategy Based on Attribute in Cloud Storage Platform [J]. Computer Science, 2016,43 (3): 167-173.

[9] Fang Dongrong, et al. Research on the Method of Deleting Data Recovery in Android System [J]. Computer Engineering, 2014,40 (10): 275-280.

[10] Xu Xianwei, Yang Yanying, Cao Ji. Analysis of File-level Data Recovery Methods in Windows Systems [J]. Journal of West Anhui University, 2014,30 (2): 24-27.