Design of Network Security Defense Knowledge Training Management Platform Under Cloud Media

Ji-yin Zhou and Chun-rong Zhou

Chongqing Vocational College of Transportation, Chongqing 402247, China
szshuishii@163.com, xumxuii2255@163.com

Abstract. With the continuous progress of Internet technology, more and more people are getting information through the network, so the number of cloud media is increasing, which brings great hidden danger to the network security. However, the traditional training management platform is difficult to deal with massive data, which leads to the imbalance of defense knowledge system in the platform and the instability of platform feedback. Therefore, a new network security defense knowledge training management platform is designed. By setting the balance constraint index, optimize the load balance layout of the training management platform; build the service framework of the training management platform, obtain the training user clustering results; set up training courses, realize the design of the network security defense knowledge training management platform. The test results show that compared with the traditional design platform, the stability of the designed platform is higher under the condition of massive network security defense knowledge. It can be seen that the designed platform is more in line with the basic requirements of network security defense.

Keywords: Cloud media · Network security defense · Knowledge training management platform

1 Introduction

With the development of Internet technology and the rise of social network, the media presents the trend of fragmentation. Everyone has become a media. This media can disseminate information and distribute information. It is displayed in personal blog, micro-blog, space home page, group and so on. At the same time, some enterprises and institutions have similar tendencies in QQ group, website, official micro-blog and WeChat official account, and all kinds of Internet applications, games and websites are showing. Interactive communication function, the collection of human media and these fragmented media, is called cloud media. Network security refers to the use of various technologies and management measures to ensure the normal operation of the network system, so as to ensure the availability, integrity and confidentiality of network data [1].

© ICST Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2020
Published by Springer Nature Switzerland AG 2020. All Rights Reserved
S. Liu et al. (Eds.): eLEOT 2020, LNICST 340, pp. 103–114, 2020.
https://doi.org/10.1007/978-3-030-63955-6_10
In response to the above problems, traditional training management platforms have set up key information and developed platform search programs to achieve reliable feedback on network security defense data. However, due to the increasing number of cloud media and the emergence of network attack methods, the amount of data on network security defense knowledge has increased. Traditional platforms have been unable to meet the training requirements. Therefore, a new network security defense knowledge training management platform is proposed. The emergence of this platform makes up for the shortcomings of traditional design platforms, and provides more rigorous technical support for national cyber security education and training [2].

2 Design of Network Security Defense Knowledge Training Management Platform Under Cloud Media

2.1 Set Balance Constraint Indicators

According to the amount of network security defense knowledge training tasks, the training management platform needs to balance the distribution and control of these training tasks by setting balance constraint indicators, so as to achieve the optimal layout of training management platform load. The unequal probability task allocation balance is mainly composed of front-end distribution and end service, so a description model is built according to this condition. Assuming that there is no connection between the distributor and the server, that is, the former does not know the load information and task quantity of the latter; at the same time, by default, the end servers can assign tasks to each end server according to a certain probability. Set the number of end servers connected to the management platform to \( n \), and the probability mentioned is represented by the letter \( p_n \), where \( 1 \leq n \leq N \) exists, \( \sum_{i=1}^{m} p_n = 1 \) exists. Let the Poisson flow of the task reach the distributor be \( \gamma \), then at this time reach the end of the Poisson flow of the server \( n \) with the parameter \( \gamma p_n \). At the same time, ensure that the training task time is subject to the general allocation, and match according to the order of queuing rules, and require that the data arrival process and service process are independent of each other [3].

The training task distribution function is known as \( f(x) \), and the training task is divided into \( N \) disjoint intervals, that is, \( [0, \infty) = [u_0, u_1), [u_1, u_2), \ldots, [u_{N-1}, u_N) \), where \( u_0 = 0 \) and \( u_N = \infty \). The dispatcher quickly assigns the task \( u_N \) to the server according to the probability \( p_n \). When the server receives the dispatcher’s task, it analyzes the training workload. When \( u_{n-1} \leq u < u_n \), the end server places the training task in the queue and waits for service; otherwise, the server returns the task, and the dispatcher reassigns the task to server \( n \), which satisfies the task assignment condition \( u_{i-1} \leq u < u_i \).

On the basis of setting the assignment conditions, set the control conditions for task assignment. It is known that the capacity of the end server is \( c \), and there is a connection between the front-end distributor and the end server. Let \( C_1 \) and \( C_2 \) represent the control programs in the two end servers. When \( C_1 - C_2 \geq \lambda \), the distributor directly assigns tasks to \( C_2 \), and the new tasks are in The \( C_2 \) server waits in line, while \( C_1 \) does not accept training tasks temporarily; when \( C_2 - C_1 \geq \lambda \), the front-end distributor assigns
training tasks to \( C_1 \), new tasks wait for services in \( C_1 \), and \( C_2 \) temporarily does not accept new assignment tasks; when condition \( |C_2 - C_1| < \lambda \) exists. At the same time, the distributor distributes system tasks to \( C_1 \) and \( C_2 \) at the same time, so that the services of the end server are performed simultaneously. The distribution and control curve of network security defense knowledge training tasks is shown in Fig. 1 below [4].

According to the above figure, the distribution curve distributes the system task amount evenly, and the control conditions are based on the control law to reasonably control the task allocation amount within a certain range to ensure the distributed parallel computing capability of the distributed management platform. The control conditions are based on the balanced distribution of training tasks, the characteristics of tilted data in the training platform are extracted, and the balance constraint index is set. The setting of this indicator allows the training management platform to run smoothly under normal load conditions, control the degree of data inclination, and make the platform’s processing result of defensive knowledge to be optimal.

Suppose the total amount of inclined data in defense knowledge is \( w \), where the data characteristics corresponding to \( w_i \) are represented by \( s_i \). The load balancing algorithm is used to calculate and classify the constraint indicators. The indicators in Table 1 below can be used as candidates.

The data in the above table includes the obtained values of alternative indicators. An index function is established to calculate the load of each node of the defense knowledge cluster on the distributed platform. Take the following formula as the basic premise of constructing index function:

\[
f(w_i) = 1 - \prod_{i=1}^{n} (1 - w_i)
\]

In the formula: \( f(w_i) \) represents the indicator substitution function; combined with a set of non-negative parameter \( \varphi_i \) corresponding to the impact indicator, multiplying
Table 1. Indicators of balance constraints

| Serial number | Index name                              | Get numerical value |
|---------------|-----------------------------------------|---------------------|
| 1             | CPU utilization                         | 87–98%/ms           |
| 2             | CPU temperature                         | 40–65 °C            |
| 3             | Memory usage                            | 70–85%              |
| 4             | Platform steady state response time     | 25 ms               |
| 5             | Platform transient response time        | 12 ms               |
| 6             | Network rate                            | 55M                 |
| 7             | Disk I/O rate                           | 75–95%              |

The indicator with the calculation result of the above formula, the obtained indicator evaluation function is:

\[
\mu(g) = s_i h(x_i) \sum_{i=1}^{n} \varphi_i f_i
\]  
(2)

In the formula: \(\mu(g)\) indicates the index evaluation function; \(f_i\) indicates the importance of the corresponding influencing factors to the final target; \(s_i\) indicates the characteristics of the tilted data [5]. According to the above formula, the load constraint indicators of each distributed node in the platform are obtained:

\[
\sigma = \kappa \eta g(w_i) \omega \ln[\mu(g)]^{-\varepsilon} + c
\]  
(3)

In the formula: \(\sigma\) represents the constraint function on \(w_i\); \(\kappa\) represents the weight coefficient; \(c\) represents the supplementary parameter; \(\varepsilon\) is the balance index; \(\eta\) represents the maximum load of the system; \(\omega\) represents the load weight of the connection.

According to the characteristics of tilt data, the above formula sets a balance constraint index to realize the balance constraint on the load of tilt data connection. Based on the control conditions and constraints set up, a balanced load layout is optimized to realize the balanced control of the inclined data connection load on the training management platform. When the load balance is on the high side, the existing load balance state can be adjusted in time. Assuming that the number of labels of program \(t_i\) is load is \(n_i\), the equilibrium layout probability is obtained according to the balance constraint of formula (4):

\[
q_i = \frac{n_i}{|n^*|}
\]  
(4)

Where: \(n^*\) represents the actual number of loads in the layout area. Then the information entropy \(D_1\) can get the maximum value, that is, \(\max D_1\) is obtained. According to the results, when the load of each program on the network platform is the same, the index \(D\) of the information entropy approaches 1. It should be noted that the index \(D\) at
this time is the label coverage. Obtained under the action of $q_j$. At this time, the amount of knowledge data is small, and the optimal location of load layout is shown in Fig. 2 [6].

According to the above figure, the mathematical model at this time can balance the load when a small amount of data is skewed. It can be seen that under cloud media, the amount of network security defense knowledge is extremely large, so the amount of skewed data also increases. When the amount of skewed data is too large, the load layout needs to readjust the balance. According to the standard particle swarm and cutting function, to a cut for large tilt data processing, data, which originally should tilt left the tilt data to be processed, also bring balance constraint index, combined with particle swarm to optimize the layout, the defense knowledge under the condition of large quantity of the data, the load optimal location are shown in Fig. 3 below [7].
According to the above two sets of optimal position diagrams, it can be known that through the set constraint indicators, constraints are set on the training platform to ensure that the defense knowledge data can maintain a balanced load control balance during the tilt change process and achieve balanced control of the training management platform.

2.2 Build the Service Structure of the Training Management Platform

The construction of network security defense knowledge training and management platform under cloud media will focus on online training management and unified data. The four directions of management, diversified training implementation and comprehensive information service are to build a comprehensive training portal platform with better service performance. The specific objectives are as follows:

Establish a training management portal, formulate and track training plans and training implementation processes, and achieve unified release of training consulting. Improve the onlineization of the overall training management process, and onlineize most of the offline business. At the same time, an information service monitoring center was established to improve management decision support. Then, it is structured with the management knowledge training thinking of the management platform, providing a unified training service resource platform for network users, integrating teaching video websites and examination system resources, docking with cloud media service centers, and achieving the construction of diversified information targeted services. Portal for integrated information services. Construct a comprehensive training management platform, and form a comprehensive learning management platform service framework with curriculum learning center, teaching management center, information monitoring center, online learning center and quality evaluation center as the main content, as shown in Fig. 4 below [8].

![User authentication service](image)

**Fig. 4.** Service framework of training management platform
Based on the background and goals of platform construction, the scope of platform training task scenarios is divided, as shown in Fig. 4 above. First, the core business scenario is divided into: training services, WeChat services, forum services, and according to three core tasks, training management, training monitoring and personal information center-related business management, while training and forum services provide unified consultation for the portal center Launched, WeChat service provides users with convenient office channels; secondly, the platform authority authentication related tasks are divided into user authentication services; finally, platform training management tasks are divided into: message platform services and file services, and data function tasks are divided into data retrieval services and decision Engine services. Integrate network security defense knowledge training management resources based on the above business divisions.

Assume that the set of knowledge requirements for network security defense is $X$, and randomly select two requirements from them, record them as $x_a$ and $x_b$ respectively, and find the similarity between them.

\[
\tau_{ab} = \frac{q_i \sum_{i=1}^{n} x_{ai} \cdot x_{bi}}{\sigma \sqrt{\sum_{i=1}^{m} x_{ai}^2 \sum_{i=1}^{m} x_{bi}^2}}
\]

(5)

Use the above formula to find the degree of similarity between the demand data, and use the best domain value method to achieve fuzzy clustering of user needs:

\[
x_i^{(e)} = \frac{\sum_{k=1}^{n_e} x_{ki}^{(e)}}{\tau_{ab}}
\]

(6)

In the formula: $x_i^{(e)}$ represents the clustering result of the $i$-th sample data under the influence of $\epsilon$-type demand; $x_{ki}^{(e)}$ represents the dynamic change constant of the demand data under the action of the change factor $k$ [9] According to the service framework of the training management platform, the training service feedback program is set up. According to the above calculation steps, the fuzzy clustering of training user needs is realized.

2.3 Implementation of Training Management Platform Design

According to the service framework of the training management platform established above, and combined with the clustering results of training user needs, the design of the network security defense training management platform is realized. Select advanced network security defense personnel to compile training courses, so that the training users can start training and learning according to the process in Table 2 below, and learn the more difficult course content level by level based on the points obtained.
Table 2. Course credit standard

| Number | Course level       | Get integral |
|--------|--------------------|--------------|
| 1      | Junior course      | 100          |
| 2      | Intermediate course| 200          |
| 3      | Advanced courses   | 300          |
| 4      | Extended Curriculum| 350          |
| 5      | Practice operation | 400          |

Users are trained to learn network security defense knowledge in accordance with the sequence of courses in the above table. Only when the course credits are met, can the next stage of course tasks be carried out. The measurement formula of training integral is as follows:

\[ I = I_1 \times I_2 + \Delta I \]  \hspace{1cm} (7)

In the formula: \( I \) represents the course credit; \( I_1 \) represents the integral base; \( I_2 \) represents the integral multiplier; \( \Delta I \) represents the reward points given during the prescribed course study time, generally between 0.1-0.3 points. The following Table 3 is the standard value table of integral multiplier \( I_2 \) [10].

Table 3. Integral multiplier standard

| Grading scale | Assessment score | Multiplier |
|---------------|------------------|------------|
| I             | More than 90 points | 1          |
| I             | 90–80 points     | 0.8        |
| III           | 80–70 points     | 0.7        |
| IV            | 70–60 points     | 0.5        |
| V             | Below 60 points  | 0          |

Train users to learn network security defense knowledge in accordance with the above-mentioned processes and course management methods. So far, the design of a network security defense knowledge training management platform under cloud media has been realized.
3 Test Experiments

A comparative experiment is proposed to compare the training management platform designed this time with the training management platform under the traditional design to compare the stability of the feedback data of the two platforms. In the experiment, the designed platform was taken as experiment group A, and the platform under traditional design was taken as experiment group B. Specific experimental conclusions were drawn based on experimental test results. Figure 5 below is the test platform built for this experimental test.

In the figure, computer 1 and computer 2 are two computers with the same model and configuration, which are respectively used for the platform design of experimental group A and experimental group B. Computer 3 is a test unit, through which the training results of two groups of platforms are obtained. The basic test environment of the above three groups of computers is shown in Table 4 below.

| Computer | Hardware                     | Software       |
|----------|-----------------------------|----------------|
| 1        | CPU:BTIV2.66G Memory:256G   | Windows Server2019 |
| 2        | CPU:BTIV2.66G Memory:256G   | Windows Server2019 |
| 3        | CPU:SYD2.13G Memory:512G    | Windows XP/IE11.0 |

According to the test environment in the above table, it can be known that the hardware capacity of the three groups of computers is extremely large, which matches
the huge volume of network security defense knowledge and meets the requirements of this experimental test.

![Graph showing platform test results with 10G network security defense knowledge]

(a) Experimental group A test results

![Graph showing test results of experiment group B]

(b) Test results of experiment group B

Fig. 6. Platform test results with 10G network security defense knowledge

The training management platform is designed using two design methods. When the data volume of network security defense knowledge is 10G, the experimental test results are obtained, as shown in Fig. 6 below.

According to the curve trend in the figure above, the stability of the platform in the two designs is similar to the standard value. To ensure the universality of the experimental test, the platform under the condition of 50G network security defense knowledge was tested. The comparison results of the experimental test are shown in Fig. 7 below.
According to the above figure, under the condition of 50G network security defense knowledge, the designed management platform can still run smoothly; while under the traditional design, the stability of the platform has dropped below 8.5, far below the standard value. Comprehensive experimental test results show that the stability of the design platform is better.

4 Concluding Remarks

In order to improve the network security defense knowledge training management, this paper designs a network security defense knowledge training management platform in the cloud media environment, which solves the problem of poor stability of the traditional design management platform, provides reliable technical support for network security, and has broad application prospects.
References

1. Shamim Hossain, M., Xu, C.S., Li, Y.T., et al.: Advances in next-generation networking technologies for smart healthcare. IEEE Commun. Mag. 56(4), 14–15 (2018)
2. Lv, Y.Y., Guo, Y.F., Chen, Q., et al.: Active perceptive dynamic scheduling mechanism based on negative feedback. Proc. Comput. Sci. 131(2), 520–524 (2018)
3. Li, Y.F., Le, T., Han, Q., et al. T.: Research Notes: Distributed Shadow for Router Security Defense. Int. J. Softw. Eng. Knowl. Eng. 28(2), 193–206 (2018)
4. Liu, T., Tian, J., Wang, J.Z., et al.: Integrated security threats and defense of cyber-physical systems. Zidonghua Xuebao/Acta Automatica Sinica 45(1), 5–24 (2019)
5. Yu, H.: Platform design of sports meeting management system for regular colleges and universities based on B/S structure. Wirel. Pers. Commun. 102(2), 1223–1232 (2018). https://doi.org/10.1007/s11277-017-5178-z
6. Emanuela, C., Francesca, C., Pericle, S., et al.: Design and impact of a teacher training course, and attitude change concerning educational robotics. Int. J. Soc. Robot. 10(3), 1–17 (2018)
7. Li, J., Xing, Z., Xing, J., et al.: Design of optimized planning platform of electric boiler with heat storage to enhance wind power consumption. Taiyangneng Xuebao/Acta Energiae Solaris Sinica 39(11), 3270–3276 (2018)
8. Zhi, M.H., Lin, P., Han, H.Y., et al.: Design and implementation of augmented reality cloud platform system for 3D entity objects. Proc. Comput. Sci. 131(5), 108–115 (2018)
9. Tang, Q.Y., Zhou, Y.M., Zeng, P., et al.: Background modeling and coding of surveillance video with variable block size. Jisuanji Fuzhu Sheji Yu Tuxingxue Xuebao/J. Comput.-Aid. Des. Comput. Graph. 30(1), 138 (2018)
10. He, H., He, T., Peng, G.: Research on network service management platform for long term mechanism of sports in colleges. Wirel. Pers. Commun. 102(2), 1117–1127 (2018). https://doi.org/10.1007/s11277-017-5146-7