Education Information Network Terminal Big Data Analysis Response and Monitoring System

Lei Ma[1(✉)], Xin-yu Lv[2], and Shuai Fu[1]

[1] Beijing Polytechnic, Beijing 100016, China
malei235@tom.com
[2] School of Mathematics and Statistics, Wuhan University, Wuhan 430070, China

Absrtact. The current data analysis response and monitoring system has not established a monitoring system communication model, which leads to poor monitoring effect of abnormal data, unable to access users at the same time, and long response time of the system. Therefore, this research designs a new education information network terminal big data analysis response and monitoring system. Considering the system functions required by the educational information network terminal, the hardware structure of the system is designed. In the aspect of software design, the communication topology of educational information network terminal is established, and the system communication model is built to make the system have communication function. Then the monitoring module of educational information network terminal is designed from the perspective of server and client. The experimental results show that: in the educational information network terminal under the system, the stored information has higher security, better accuracy, processing ability and completeness, and can support more virtual users to visit the system pages at the same time, with faster response time.

Keywords: Education information network · Terminal big data · Analysis response · Data monitoring

1 Introduction

With the rapid development of computer network, computer has been widely used in various industries and fields. In order to realize the sharing of internal resources, the application of local area network has been greatly developed. In order to make better use of the functions of the Internet, more and more companies, schools and various functional departments have provided the function of interconnection with the Internet. Although this measure brings a lot of benefits to the development of education, it also threatens the security of educational information. Especially, the educational information network terminals, such as users using U-disk with virus or browsing aggressive websites, may damage their own terminal devices. If it is a worm, it will infect other devices in the network, causing serious consequences [1]. Therefore, the network terminal monitoring technology has high practical value and research significance, and the research on this technology will make up for the internal security defects of the network.

W. Fu et al. (Eds.): eLEOT 2021, LNICST 390, pp. 502–513, 2021.
https://doi.org/10.1007/978-3-030-84386-1_41

Remote monitoring is a frontier research topic at home and abroad, and active research has been carried out. Due to the rapid development of computer technology and communication technology in China, research in this field has been actively carried out in recent years, and network terminal monitoring devices such as Meiping network management master and network post have been designed [2]. However, in the above research, there are some problems, such as the poor effect of information transmission and client network information guarantee. To solve this problem, this study designed a new education information network terminal big data analysis response and monitoring system.

2 System Hardware Structure Design

The design of educational information network terminal monitoring system, considering the system function required by the educational information network terminal, and the realization of the system monitoring educational information network terminal function, based on the research of educational information network terminal monitoring system at home and abroad, determine the main structure of the system, including educational information network terminal data acquisition, data processing, data communication, LCD Among them, the core control part is the control module of the system, which controls the main operation of the system. Therefore, the hardware structure of the education information network terminal monitoring system designed this time will select pici8f87k22 single chip microcomputer with 8-bit high performance as the core controller of the system. The hardware structure of the design system is shown in Fig. 1.

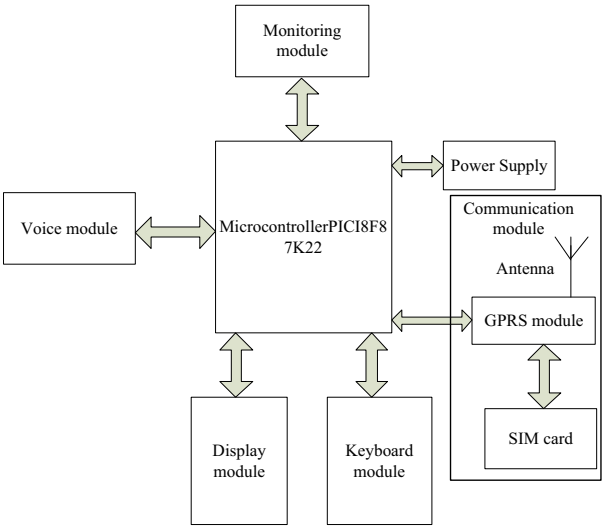

Fig. 1. System hardware structure

As can be seen from Fig. 1, the hardware structure of the system is composed of monitoring, voice, power supply, communication, display, keyboard and other modules.

Among them, the communication module is used to connect the monitoring center and system terminal equipment of the monitoring module; the voice module is used for voice alarm in the nursing process, such as large fluctuations in the educational information network terminal, abnormal data in the information stored in the educational information network terminal, etc., to prompt relevant personnel through voice broadcast; the display module is used to display the current monitoring educational information network Terminal data, such as the access and response of educational information network terminal.

3 System Software Design

Based on the hardware design of the education information network terminal monitoring system, this paper determines the education information network terminal communication topology, analyzes the education information network terminal response with big data, establishes the system communication model, promotes the system to have the communication function, and designs the monitoring education information network terminal monitoring module from the two directions of server and client, so as to ensure the education information network The terminal runs safely.

3.1 Big Data Analysis and Response of Educational Information Network Terminal

Suppose that the educational information network is a double-layer educational information network composed of wireless network and wired network [3]. There is no link between wireless network and wired network, but there is link between wired network and wired network, and between wireless network and wireless network. Among them, the wireless network is responsible for the communication with small handheld terminals, and the wired network is responsible for the relay and forwarding of signals and the communication with large terminals. The communication topology of educational information network terminal is shown in Fig. 2.

In Fig. 2, terminal A and terminal C are within the coverage of the wireless network. The communication process of terminal A and terminal C is: terminal a → wireless network → terminal C. The communication between terminal A and terminal B needs the internal routing of satellite network, and their communication business process is: terminal a - wireless network 1 → wired network 1 → wired network 2 → wireless network 2 → terminal B. According to the above analysis process, analyze the big data analysis response of education information network terminal.

The service response of educational information network terminal is defined as the time from a certain terminal to sending service request to receiving the reply from the destination terminal [4, 5]. Therefore, the service response includes two parts: the delay in the data sending phase and the delay in the receiving phase. Only interactive service has the concept of response. When the service type belongs to non interactive service, the bidirectional response of service will degenerate into one-way delay of the whole network.

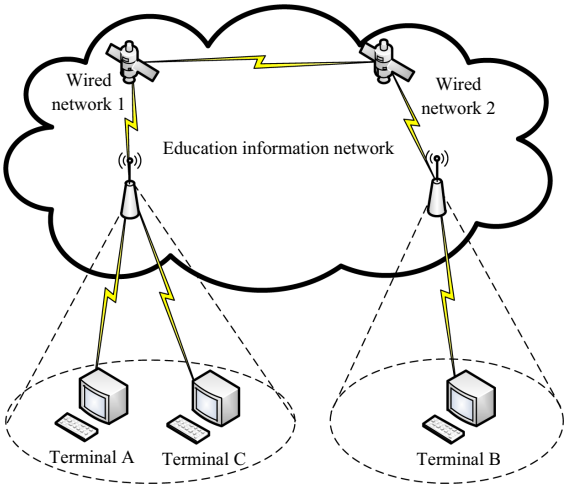

Fig. 2. Communication topology of educational information network terminal.

The service types of educational information network terminal include real-time service and non real-time service. The characteristics of real-time service are connection oriented, high delay requirement and low bandwidth requirement. The real-time service requires to complete the communication between two terminals with as low delay as possible. For non real time services, the receiving terminal may not be online, the network equipment needs to store data, and the non real time service itself does not require high delay [6]. Therefore, the analysis of education information network terminal big data analysis response, the main analysis of the terminal response to real-time business.

In the whole process, the delay in both sending and receiving stages can be further divided into terminal delay and spatial link delay. In the communication process from A to B, the sending and receiving terminals will produce packet processing delay and transmission delay respectively [7]. Space link will have propagation delay, transmission delay, processing delay and queuing delay. Then the packets returned by B are sent to terminal A according to the communication process of terminal B → satellite network → terminal A, which is similar to the response analysis from terminal A to terminal B. So far, A receives the packet replied by B, that is A's packet is responded.

3.2 Establish System Communication Model

According to the education information network terminal communication topology shown in Fig. 2, we can find that the education information network is mainly used in the internal LAN. Therefore, the design of educational information network monitoring system, mainly used in the internal LAN monitoring, then the design of the monitoring system, to complete the function design, its monitoring system communication model is shown in Fig. 3.

The communication model of the monitoring system as shown in Fig. 3 is divided into two parts: client and server. Among them, the client runs the monitoring driver and is the data source of the whole system. In order to reduce the load of the client and for

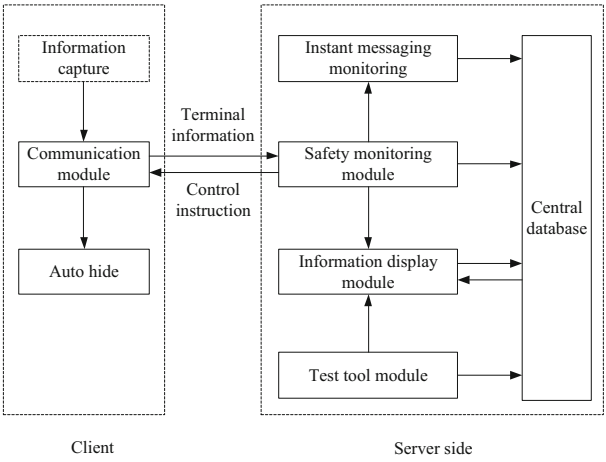

Fig. 3. Communication model of monitoring system

the consideration of security, the system adopts a centralized data management method to uniformly manage and summarize the data [8, 9]. This is easy to maintain the integrity and stability of the data, but also conducive to the server quickly retrieve and display data.

3.3 Monitoring Education Information Network Terminal Monitoring Module

Based on the above design of the education information network terminal big data analysis response and communication module, we can find that the design of the monitoring system, the education information network terminal, are divided into server and client two aspects, so, this section of the design of education information network terminal monitoring module, also from the server and client two aspects, monitoring education information Information network terminal.

1. The client consists of the message part and the request processing function initiated by the local receiving server. Through the interaction between these function lists, the integrity of the whole system can be guaranteed. The client mainly includes the following parts:

   (1) Information capture part: mainly responsible for collecting the key system information (CPU (Central Processing Unit), memory, process list, etc.) on the host;
   (2) Communication module: the main function is to receive instructions or messages sent by the server, make corresponding responses, such as locking or unlocking, shutdown and other instructions, and realize encrypted communication with the server;
   (3) Hidden module: mainly responsible for the automatic loading of the client and the automatic hiding of the corresponding process [10].

2. The server is composed of security monitoring, information display, communication, system maintenance tools and other functions. Through the interaction between these function lists, the system has the monitoring function. The specific functions are as follows:

   (1) The security monitoring module includes: LAN (Local Area Network) scanning processing module, port summary processing module, filter analysis processing module, port log processing module, firewall processing module, etc. The monitoring server dynamically analyzes all the incoming and outgoing IP (Internet Protocol) addresses and ports in the LAN. According to the abnormal analysis of the ports and incoming and outgoing packets, the illegal operation can be judged. Summarize the ports by IP address to view the illegally used network processes. The abnormal IP address can be analyzed separately to determine the main object of illegal operation. Firewall can be used to block the port and address.
   (2) Information display module includes: screen capture processing module, client locking module, communication processing module, client management module, etc. It mainly monitors the client on a regular basis, and remotely captures the abnormal traffic. The client can directly view the screen. If illegal use is found, the message module will give a warning. If you don't pay attention to it, you can lock the client or remotely close the client.
   (3) Instant messaging module. Mainly for the use of abnormal time, such as MSN (Microsoft Service Network) for content and message capture.
   (4) The integration tool module includes: routing test and connectivity test. Using these tools to test the connectivity of local LAN and the function of remote network routing, the administrator can quickly find the cause of network failure.
   (5) Central database. It mainly stores and manages all kinds of data, and is the storage center of system monitoring data.

4 Experiment and Result Analysis

In order to verify the feasibility of the big data analysis response and monitoring system designed above, the following experiments are designed.

By means of comparative experiment, the big data analysis response and monitoring system of the educational information network terminal designed in this paper is recorded as System A, and the traditional system is recorded as System B. Then determine the number of intrusion data of educational information network terminals, change the number of system access and login, and compare the effect of abnormal data monitoring, access speed and system response time of the two groups of systems.

4.1 Experimental Preparation

The experiment is based on the Visual Studio development platform, and the remaining development environment parameters are shown in Table 1.

Table 1. Two groups of system development environment

Environmental Science	Configuration	Parameter
Software	Programing language	C++
	Operating system	Windows 10
	SERVER network	Wired network
	Network IP address	127.0.0.1
	LDAP (Light Directory Access Portocol) management	Phpldapadmin
Hardware	LDAP server	OPENLDAP
	Hard disk	40G
	Web server	Internet Information Server, IIS

In addition, the baud rate of the experimental communication protocol is set to 9600 bps, and the receiving and sending codes of the information are ASCII (American Standard Code for Information Interchange) codes.

Based on the above content and considering the transmission efficiency of the data transmission protocol, the mesh topology structure is selected as the topological result of the experimental method. The topology is shown in Fig. 4.

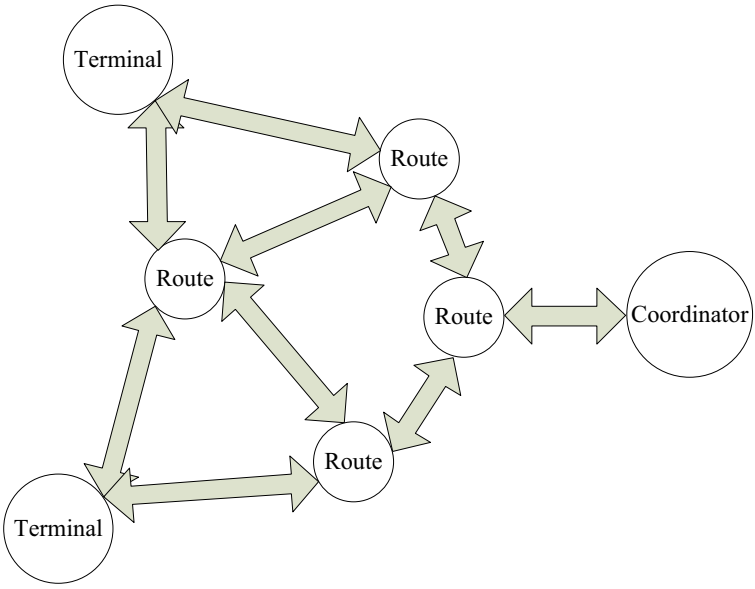

Fig. 4. Topological structure of two groups of system operation environment

4.2 Experimental Result

The First Group of Experimental Results

The first group of experiments was carried out based on the experimental parameters set above. Considering that a large amount of network education information is stored in the education information network terminal, the designed network education terminal monitoring system needs to have the function of monitoring information security. Therefore, set the abnormal data as shown in Table 2 and distribute it to the education information terminal to attack the education information stored in the education information terminal.

Table 2. Abnormal data

Data name	Quantity/piece	Data name	Quantity/piece
DOS	6295	U2R	69
P2L	979	PROBE	2806
Number of normal data			831974
Total number of abnormal data in KDD cup 1999			842123

In order to make the experiment more authentic, the educational information stored in the educational information terminal is divided into three sets. In order to reduce the difficulty of the experiment, the abnormal data shown in Table 2 is evenly distributed to the education information set stored in the education information terminal, which accounts for 1% of the total number of the education information set stored in the education information terminal. In this experiment, the attack type data distribution results are shown in Table 3.

Based on the abnormal data shown in Table 2 and Table 3, select the detection rate and the false alarm rate, verify the big data analysis response and monitoring system of the Yu Information Network Terminal, and monitor the security accuracy, processing capacity and completeness of the information stored in the Yu Information Network Terminal Therefore, the expressions of the detection rate D and the false alarm rate F of the information security of the education information network terminal are:

$$\begin{cases} D = \dfrac{m}{M} \times 100\% \\ F = \dfrac{e}{E} \times 100\% \end{cases} \tag{1}$$

In formula (1), M represents the total number of intrusion data; m represents the number of detected data intrusions; E represents the total number of events; e represents the number of false alarm events. At this time, change the total number of test data and the number of abnormal data intrusion, record the number of detections and false alarms of the two systems, and use the formula (1) to calculate the detection rate and false alarm rate. The experimental results are shown in Table 4 Show.

Table 3. Distribution of abnormal data

Data	Aggregate 1	Aggregate 2	Aggregate 3	Intrusion type
Rootkit	9	10	6	U2R (User-to-Root)
Loadmodule	9	21	14	U2R
Warezmaster	48	37	170	R2L (Remote-to-Local)
PSpy	48	0	31	R2L
Multihop	52	252	92	R2L
Ftp-write	45	116	108	R2L
Portsweep	29	154	439	PROBE
Ipsweep	54	350	1780	PROBE
Smurf	73	529	1353	DOS (Disk Operating System)
Neptune	185	524	317	DOS
BACK	315	2514	697	DOS

Table 4. Comparison table of the monitoring results of the two groups of systems

Test	5489		3978	
Invade	1852		1278	
System	A	B	A	B
monitor	1756	1531	1191	905
D/%	94.82	82.67	93.17	70.81
False positive	181	208	101	137
F/%	3.29	11.23	2.97	10.71

It can be seen from Table 4 that the information stored in the B system monitoring education information network terminal is safe, and the detection rate and false alarm rate obtained by its monitoring increase with the increase of the number of intrusions, which has a better detection effect. However, the average detection rate is 80.36%, the overall intrusion detection rate is low, the average false alarm rate is 10.3%, and the overall false alarm rate is high. System A monitors the security of the information stored in the education information network terminal, and its monitoring The detection rate and false alarm rate obtained vary with the total number of tests, and it also has a better detection effect. However, the average detection rate is 93.79%, which is significantly higher than the B system, and the average false alarm rate is 3.11%, significantly lower than the B system. It can be seen that the big data analysis response and monitoring system of the education information network terminal designed this time monitors the security of the information stored in the education information network terminal, and has better accuracy, processing capacity and completeness.

Second Set of Experimental Results

In the second group of experiments, considering the system monitoring the running state of the educational information network terminal, the security data of the running state is obtained. Due to the existence of multiple simultaneous access to the phenomenon, will affect the system page access speed. Therefore, compare the two groups of system page access speed. In this group of experiments, a total of 300 users are simulated and the system functions are accessed at the same time. Every 1 min, 30 virtual users are added, and the response time of the above five functions is recorded under different numbers of virtual users, and the 5 functions are calculated The average response time is shown in Fig. 5.

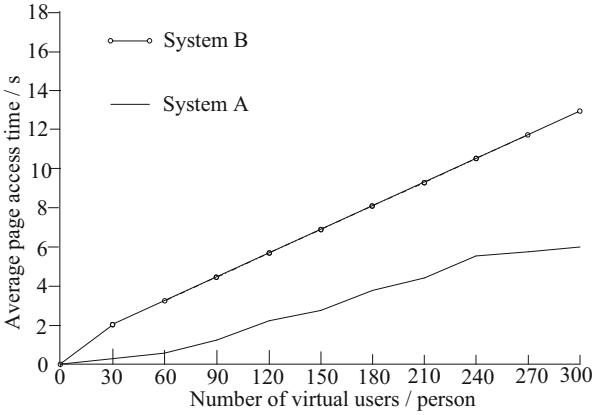

Fig. 5. Two sets of system page access speed test results

It can be seen from Fig. 5 that as the number of virtual users increases, the average time to access system functions increases. Although the B system can support 300 virtual users to access the system pages at the same time, when the number of users continues to increase, based on the current trend, the average page access time is proportional to the number of virtual users; A system, when virtual users When it reaches 240 people, the average page visit time is close to a straight line, and it is impossible to judge how many virtual users can be supported to visit the system page together. It can be seen that the big data analysis response and monitoring system of the Yu Information network terminal designed this time can support more virtual users while accessing the system page, and the average access time of the system page is only 8 s.

Results of the Second Set of Experiments

Based on the results of the first set of experiments and the second set of experiments, the second set of experiments is carried out. In the system, 500,000 user records are preset. At this time, the Loadrunner stress test tool is used to simulate 600 logged-in users. Let these 600 simulated users load a user trend every 3 s until the 600 simulated users are loaded. The initial statistics of virtual users are 100 virtual users. Users, log in and operate the system at the same time, and the execution time of each user's operation

lasts for five minutes. According to the operation process of the above settings, the system response time should be maintained within 3 s (including 3 s) when the system is operated by the user under normal conditions. According to the experimental process of this set of experiments, the response time test results of the two systems are shown in Table 5.

Table 5. Terminal response time test results

System	Test items	
	Number of concurrent users/a	System response time/s
System A	50	0.2
	100	0.6
	150	1.3
	200	1.8
	250	2.3
	300	3.0
System B	50	3.1
	100	5.5
	150	6.2
	200	7.7
	250	8.1
	300	8.9

It can be seen from Table 5 that the response time of system B is the longest of the two groups of systems, and can only support less than 50 virtual users while using the system; system A has the shortest response time and remains within the normal range. It can be seen that the education information network terminal big data analysis response and monitoring system designed this time can support 300 people to log in to the system at the same time, and the system has the shortest response time.

Based on the above three sets of experimental results, it can be seen that the big data analysis response and monitoring system of the education information network terminal designed this time can support more virtual users and access the system page at the same time, and the system response time is the shortest. Among the monitoring education information network terminals, The stored information is safe, with better accuracy, processing capability and completeness.

5 Conclusion

This study design education information network terminal data analysis response and monitoring system, on the basis of the present study, from the education information

network terminal client and server two aspects, the structure design and function module division, improve the education information network terminal data analysis response and monitoring system for monitoring capability. However, the education information network terminal big data analysis response and monitoring system designed this time did not consider the relationship between the system and the client, firewall, anti-virus and other software. Therefore, in future research, it is necessary to further study the education information network terminal big data analysis response and monitoring system, and coordinate the relationship with each other, so as to avoid the appearance of system instability.

Project: Personal information security threats and Countermeasures under the background of big data.

References

1. Song, X.: Design study of underground power supply network monitoring system in Sanyuan Coal Industry. Coal Chem. Ind. **43**(8), 71–73 (2020)
2. Wang, T., Zhu, Y., Zhao, W., et al.: Research on alarm generation algorithm of visual monitoring system integrating Bayesian network. China Comput. Commun. **32**(10), 23–25 (2020)
3. Tang, Z.: Dynamic integration simulation of multimedia network video surveillance front-end data. Comput. Simul. **37**(4), 155–158+465 (2020)
4. Yang, Y.: Design and application of computer video monitoring system. China Comput. Commun. **32**(12), 101–103 (2020)
5. Li, H.: Design of automation monitoring system for real-time sensitive information of electrical equipment. Mod. Electron. Tech. **43**(4), 1–3, 7 (2020)
6. Wu, J.: Design of network data flow intelligent monitoring system based on operation and maintenance data. Bull. Sci. Technol. **35**(7), 156–160 (2019)
7. Shi, G., Xu, J., Guo, Q., et al.: Design and implementation of location monitoring system based on mobile terminal. Inf. Res. **45**(5), 61–65 (2019)
8. Fu, W., Liu, S., Srivastava, G.: Optimization of big data scheduling in social networks. Entropy **21**(9), 902 (2019)
9. Liu, S., Glowatz, M., Zappatore, M., et al. (eds.): E-Learning, E-Education, and Online Training, pp. 1–374. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-93719-9
10. Liu, S., Li, Z., Zhang, Y., et al.: Introduction of key problems in long-distance learning and training. Mob. Netw. Appl. **24**(1), 1–4 (2019)