Construction of a Gateway Boundary Security Protection Platform Based on the Internet of Things and Cloud Computing

Chen Cheng(✉), Siyao Xu, Mingyang Peng, Ziying Zhang, and Yan Li

Electric Power Research Institute of Electrical Guangdong Power Grid Co., Ltd., Guangzhou 510080, China
cchustdky@163.com

Abstract. In view of the problems of long warning time and poor protection effect of traditional gateway boundary security protection platform, a gateway boundary security protection platform based on Internet of things and cloud computing is designed. Net FPGA chip is used for the verification and development of network communication equipment, connecting the ATA serial port connection line port of multiple boards. Combined with the register host computer, the read-write operation of the registers inside each module in the hardware is completed through PCI bus, and the hardware design of the gateway boundary security protection platform is completed. Establish the gateway border security protection module and complete the software design of the gateway border security protection platform. Based on the Internet of things and cloud computing technology, match the network security link, so as to realize the security protection of the network boundary. The experimental results show that the security protection effect of the platform constructed in this paper is better, and can effectively shorten the security early warning time.

Keywords: Internet of Things · Cloud computing · Gateway boundary · Security protection platform

1 Introduction

Network boundary refers to the boundary between our network and other networks. At present, the widely used network boundary security device is firewall [1]. The firewall can control the traffic in and out of the network boundary according to the preset security policy, but the firewall lacks the analysis and detection function of the traffic in and out. Although the intrusion detection platform proposed later makes up for this deficiency, the intrusion detection platform is a passive security device. It only analyzes whether the incoming and outgoing traffic contains attack messages, but can not process the messages containing attack information. Corresponding measures can be taken only when the network administrator sends the alarm information of the intrusion detection platform, at this time, the intruder may have already completed the network intrusion

S.-H. Wang and Y.-D. Zhang (Eds.): ICMTEL 2022, LNICST 446, pp. 43–57, 2022.
https://doi.org/10.1007/978-3-031-18123-8_4

[2]. Network boundary security protection platform is an intelligent security platform, which can not only detect the occurrence of intrusion, but also stop the occurrence and development of intrusion in real time through closed-loop response, so as to protect the information platform from substantive attacks [3].

Network boundary security protection platform is an active and active intrusion prevention and blocking platform. It can detect and intercept intrusion activities and aggressive network traffic in real time to avoid any loss [4]. The platform is deployed at the boundary of the network. When an attack attempt is detected, it will automatically throw away the attack packet or take measures to block the attack source. Although the network boundary security protection platform is similar to Intrusion Detection System (IDS) and firewall in some aspects, it is a new security technology integrating detection and access control. The analysis and detection function of the network boundary security protection platform is similar to that of IDS, but it is connected to the network in series, and the detection methods and strategies are adjusted according to the special requirements of protection, balancing the characteristics of false positives and false positives [5, 6]. Reference [7] proposed to build a zero trust security protection system in the environment of power Internet of things. The characteristics of boundary protection model commonly used in network security protection are analyzed. Aiming at the problem of insufficient security protection ability of the model, a security protection model of power Internet of things network based on zero trust security architecture is proposed. The application of zero trust in power Internet of things is analyzed and studied. This method has certain effectiveness, but the safety protection effect is poor. Reference [8] proposed an endogenous security protection framework suitable for 5G MEC in power industry. According to the characteristics of power 5G MEC, this paper proposes an endogenous security protection framework suitable for power 5G MEC, which can effectively resist various security threats, but the security early warning time is long.

To solve the above problems, this paper constructs a gateway border security protection platform based on Internet of things and cloud computing. This paper designs the hardware of gateway boundary security protection platform through net FPGA chip and register. Based on the Internet of things and cloud computing technology, the gateway boundary security protection module is established, and the gateway boundary security protection platform software is designed to match the network security link, so as to realize the security protection of the network boundary. The platform can effectively improve network security, shorten the security early warning time, and provide conditions for the development of network security.

The Internet of Things (IoT) is a variety of terminal perception devices with some perception, processing and control capabilities installed in real life entities. It uses the network to complete information interaction, processing and coordination in order to achieve large-scale data exchange between things and people, things and things. Its ultimate goal is to use the network to complete the mutual communication and communication between people and things, things and things, and all objects, so as to facilitate identification, control and management [9]. Its related technologies have considerable development prospects in national defense and military industry, industrial control, public facilities, medical assistance, smart grids, smart cities, smart transportation, and

environmental monitoring. Cloud computing is a delivery and usage model of software/hardware services. Cloud computing service providers use the network to provide software/hardware resources as services to users in accordance with the user's platform requirements. Among them, "cloud" serves as the software/hardware resources on the server cluster on the network, such as hardware resources (central processing unit, Storage, Servicer, etc.) and software resources (Application Program, operating platform or compilation platform, etc.). The client device only needs to after sending the request, the cloud computing platform can integrate the software/hardware resources on the Internet of Things to provide corresponding services and return the final calculation results to the client device. In this way, the client device can get far beyond its own computing power [10]. In recent decades, due to the emergence of IoT sensing technology and cloud computing technology, it is possible to install a variety of terminal sensing devices with recognition capabilities, processing capabilities, and control capabilities in physical entities, which will sense data through the network. Transfer to the server for storage, identification, analysis, management and control. For all walks of life, there are many types and numbers of terminal sensing devices, and massive amounts of sensing data are collected. Computing these massive amounts of data requires computing devices with huge processing capabilities. Cloud computing, as the basis for the Internet of Things technology to complete massive data processing, provides processing support for the massive information data collected by the Internet of Things platform [11]. There are many possibilities and problems to be solved in the combination of Internet of things and cloud computing. Scale: scale is a prerequisite for the combination of cloud computing and the Internet of things. Only when the scale of the Internet of things is large enough can it be combined with cloud computing, such as industry applications: smart grid, seismic network monitoring and so on. For general, local and home network IOT applications, it is not necessary to combine cloud computing. How to make them develop to the corresponding scale remains to be solved.

2 Hardware Design

2.1 Net FPGA Chip

Net FPGA chip is mainly used for verification and development of network communication equipment, and it has abundant resources for researchers to develop high-speed Ethernet equipment. There are four RJ45 high-speed Ethernet ports, supporting Cat5E or Cat6 standard cables, two 2.25MB SRAM, two 32MB DDR2 DRAMs, and two ATA serial ports that can connect multiple boards. The user is the logic core, an international test port, and the IP core of the PCI interface is solidified in the chip. The chip parameters are shown in Table 1.

As shown in Table 1, Net FPGA chips have high-speed and large-capacity peripheral storage space and programmable Gigabit physical network interfaces, and provide reference design projects such as four-port network cards, routers and switches [12]. Description language engineering package. The design code in the engineering package configures the main chip through the PCI interface after the integrated wiring, so as to realize the designed platform function. Among them, stanfor's DEMO has three

Table 1. Chip parameters

Resources name	Remark	Quantity
Slices	Logic piece	23616
SliceFlipFlops	Deposit	47232
4 input LUT	Input lookup table	47232
Bonded IOBs	External IO	692
BRAMs	RAM on chip	232
GCLKs	Global clock	16
DCMs	Clock management	8

projects, namely four-port network card and gigabit switches and Linux-based hardware-accelerated routers with simple routing protocol (PW-OSPF), these three projects fully reflect the idea of modular design, that is, develop within the same framework and use the same data and register pipeline [13], the reference design only needs to re-develop individual modules to achieve different platform functions. This unified basic design framework is also the design basis for the subsequent development of Net FPGA chips. The platform designed in this article is designed with reference to the router project as the basic framework. Among them, the physical resources of the Net FPGA chip have four physical ports, corresponding to four Gigabit Ethernet ports, which are called MAC0MAC3 in platform engineering. The other four CPU queues, the CPU0CPU3 queue ports correspond to the device drivers of the operating platform, and they mainly realize the transfer of data packets to the host computer through the PCI bus. In the User_data_path module, the core processing module of the platform, the Input_arbiter module completes the round-robin reception of data packets in eight different queues. The Output_port_lookup module is mainly responsible for determining the output port of the transmitted data packet. The Output_queue module is responsible for the round-robin transmission of data packets in eight different queues. The principle is shown in Fig. 1.

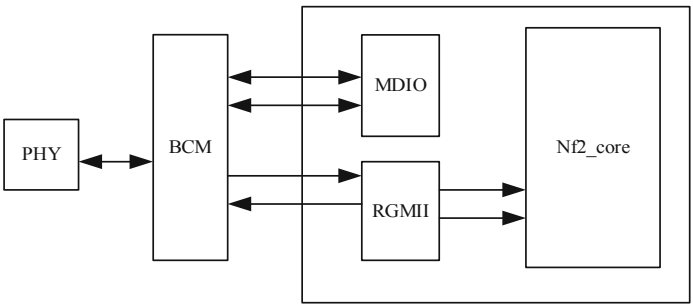

Fig. 1. Chip principle

As shown in Fig. 1, in the physical layer interface module, in order to reduce the internal clock of the platform, an RGMII interface module is added inside the FPGA. This module combines the original 4-bit network data of the network into 8-bit data and then goes to the next stage. Module transfer, MDIO module is responsible for the configuration of Gigabit Ethernet data input and output functions. The platform configures the Net FPGA chip and the internal registers of the platform realizes the programming of the external chip, so as to achieve the control of the data transmission function.

2.2 Register

The function of the register pipeline is to enable the host computer to complete the read and write operations of the internal registers of each module in the hardware through the PCI bus, so as to realize the functional configuration of the hardware module or read the relevant data information of the hardware module. The internal registers of the hardware module are divided into two types in the design of this platform: The first type is software registers, which can be read and written by the upper computer, while the hardware modules can only read operations on them. This type of register is mainly used for module functions. The second type is the hardware register, which can be read and written by the hardware, while the software can only perform read operations on it. This type of register functions mainly to realize the hardware counting function and is mainly used to record the flow information through the module. The register interfaces are all bidirectional bus signals, which can simultaneously receive the register data signal from the previous module and complete the backward transfer of the register signal of this module. In terms of register configuration, the Net FPGA project provides users with upper computer device driver functions, including hardware register read and write operation functions (regread, regwrite). Developers can use these two functions to implement hardware registers. The entire operation process of the read and write access operation is as follows: first, the user sends out a read and write signal, the addressing bit width of the read and write signal is 27 bits, and 32 bits can be read or written each time, and then the data passes through the operating platform the device driver function converts the user request into a register pipeline signal and sends it to the Net FPGA chip. Each module of the register is transferred until the register module with the corresponding address is found. After the write operation is completed, the data is sent back to the operating platform along the same path.

3 Software Design

3.1 Establish a Gateway Border Security Protection Module

In the platform designed in this paper, besides the hardware design, the software design is very important. Based on this, this paper designs a security protection module for the gateway boundary. The working principle of the simple message filtering module is to judge whether the network message is allowed to enter and leave the network by checking and comparing some information in the header of the network message, without

checking the content of the network message [14]. The simple message filtering module uses the information in the header of TCP / IP protocol message, such as protocol type, source IP address, destination IP address, TC or UDP port, to determine whether the network message can pass through the network boundary. A simple message filtering function is embedded in the filter table of Netfilter in Linux 2.4 kernel. A simple packet filtering module can block some unsafe network access at the network boundary.

Stateful message filtering module. Connection tracking (CONNTRACK) is mainly used to track and record the connection state, and realize the transition between states, and it also saves the communication information of each session. CONNTRACK does not register any rule table, indicating that it does not need rules to determine whether to do connection tracking. The connection here does not only refer to the TCP protocol connection, it also includes the UDP protocol and the ICMP protocol. Of course, this is only the protocol included in the standard implementation of the kernel. The connection trace of other protocols can be added to the kernel itself. Connection tracking is the basis of address translation. This module must be loaded when using the address translation function. The platform only processes the first message of a connection (TCP or UDP), and then relies on the connection tracking mechanism to complete the processing of subsequent messages. Connection tracking is a mechanism that can be used in conjunction with NAT to process actions related to higher-level protocols at the transport layer (or even the application layer). There are many components in CONTRACK to handle TCP, UDP or ICMP protocols. These modules extract detailed and unique information from network messages, so they can keep track of every data stream. This information also determines the current state of the CONNTRACK stream. For example, UDP streams are generally uniquely determined by their destination address, source address, destination port, and source port. In the control table, the message is related to the four different states of the traced connection. They are NEW, ESTABLISHED, RELATED, INVALID, the following is the description of these states. NEW—It means that this message is the first message of a connection. ESTABLISHED-Indicates that a connection has message transmission in both directions. The connection in the ESTABLISHED state is very easy to understand. As long as the response is sent and received, the connection is in the ESTABLISHED state. To change a connection from NEW to ESTABLISHED, it only needs to receive a response message. Using the above state information to filter network messages, the state-based filtering function can be realized. This will make the network border protection platform very strong and effective. For example, when there is no state mechanism, it is often necessary to open all ports above 1024 to release the response data. Using the state mechanism, you can only open those ports that have response data, and all other ports can be closed, which enhances the function of platform protection.

The network address translation (NAT) module is used to realize the conversion between internal network addresses and public network addresses, and the NAT table of Iptables implements this function. This module can perform one-to-one, one-to-many, and many-to-many network address conversion tasks for network messages. NAT was originally a solution proposed to solve the shortage of P address space, but it hides the internal network topology from the outside, forming an invisible boundary between the internal network and the external network, so that external hosts cannot actively access the network. Internal nodes, thereby improving the security of the internal network.

The protocols supported by the NAT module include IP, ICMP, UDP, TCP, etc. There are 3 types of NAT: static address translation, dynamic address translation, and port address translation. The NAT module in the Netfilter framework contains three built-in hook chains: NF_P_LOCAL_OUT, NF_IP_PRE_ROUTINGNF_IP_POST_ROUTING. The NAT table supports the following NAT types: SNAT: Change the source address of the data packet. DNAT: Change the destination address of the data packet. M.ASQUERADE: Belongs to a special form of SNAT. Realize the P address camouflage function. REDIRECT: A special form of DNAT. It is used to change the destination IP address of a qualified network message to the I address of the network interface when the network message enters the platform.

The analysis and detection module obtains network messages from the network protocol stack and analyzes whether there is an attack event. Analyze the content and characteristics of the attack through techniques such as feature matching, traffic analysis, protocol analysis, and session reconstruction. The results obtained through analysis and detection are submitted to the response module, and the response module executes the corresponding response action, and submits the message containing the attack information, the analysis result of the attack event, and the response strategy to the log platform for storage, so that the network administrator can view it afterwards.

The function of the closed-loop response module is to judge whether the network message passes through the network boundary in real time according to the detection results of the analysis and detection module. Because there are some false alarms in the analysis and detection module, in order to reduce the impact on the normal network operation, the response of the closed-loop response module must be classified. This platform is divided into three categories. One is to only send out alarm (Alert) information, the second is to drop the message when it is more dangerous, and the third is to send a response message when it is the most dangerous. Such as Tcp-reset packet to cut off the connection (Reject). Each specific detection rule controls whether to perform a closed-loop response. The specific method is to use the first keyword of the rule to distinguish. If the keyword in this part is Drop, it means that the rule is matched and the report is discarded. The text and send out the alarm information; Alert means that the rule is matched and only send out the alarm message; Reject means that the rule is matched and send out a response message and send out the alarm message. The closed-loop response module is implemented by the Target module in Netfilter. As the analysis and detection module is Netfilter's Match module, Netfilter calls the Target module to respond to the message according to the detection result of the analysis and detection module.

The analysis and detection module generates corresponding alarm information when a network attack is detected. These alarm messages are generated in the Linux kernel, and they need to be transmitted to the user space through a certain mechanism, and then the user space daemon processes the alarm messages. The usual practice for these alarm information is to store these alarm information in the log file of the platform so that the network administrator can view and analyze the alarm information. There are many ways to exchange information between the Linux kernel and the user space. This platform uses the Linux Netlink mechanism to complete the transmission of the alarm information of the analysis and detection module.

After adding the relevant kernel module options to the kernel, the Iptables software used in the user space must provide the relevant command line options. The analysis and detection module in this platform is implemented in the way of Match module expansion, so the program used in user space must also be provided. In order to make each extension module use a version of Iptables software without having to write a specific software version of the related extension, Iptables adopts a shared library to solve this problem. The shared library has the function of init (), which is similar to the function of the kernel module. It is called automatically when loading. This function calls register according to the new match added_match(), a shared library can provide the functions of initializing data structures and providing related options. The main data structure used in writing shared libraries is iptables_ Match, which is passed to register as a parameter_match() registers the relevant command-line matching options to let iptables recognize the new match. Through the establishment of the protection module of the platform, the safety performance of the platform can be initially guaranteed.

3.2 Matching Network Security Links Based on the Internet of Things and Cloud Computing

Cloud computing enables computer system resources, especially storage and computing capabilities, to be provided on demand without the need for users to directly manage them actively. Cloud computing is usually used to indicate that many users can use the data center through the Internet of Things. The large clouds that dominate today have the ability to distribute from a central server to multiple locations. If the connection to the user is relatively close, it can be designated as an edge server. The cloud can only serve a single organization (private cloud), it can serve many organizations (public cloud) or a combination of the two (hybrid cloud). Therefore, this article combines cloud computing with the Internet of Things to create a secure protection link for the network boundary.

In order to better improve the security of the network, this paper uses the network similarity measure for cloud computing, and uses the Euclidean distance to unify the calculation results, as shown below:

$$d = \sum_{i=1}^{N} \sqrt{(X_{1i} - X_{2i})^2} \tag{1}$$

$$A = \sum_{p} \left\| I_1^p - I_2^p \right\| \tag{2}$$

$$d' = \max(|x_1 - x_2|, |y_1 - y_2|) \tag{3}$$

$$J = \frac{dx_i y_i}{\sqrt{\sum x_i^2} \sqrt{\sum y_i^2}} \tag{4}$$

In formula (1–4), d is the Euclidean distance from the network information transmitting end X_{1i} to the receiving end X_{2i}; N is a constant; A is a unified vector parameter; I_1^p and I_2^p are different boundary coordinates; p is the attribute measurement index; x_1,

x_2, y_1 and y_2 are coordinate values of different network nodes; d' is the distance after unification. J is the included angle of space vector; x_i and y_i are network node similarity indicators. Taking $d(i, j)$ as the network boundary node, the ratio of network security is as follows:

$$D = \frac{\min_{1 \le i \le j} d(i, j)}{\max_{1 \le k} d'(k)} \tag{5}$$

$$\delta_i = \min d_{ij} \tag{6}$$

In formula (5–6), δ_i is the network sensitive value; i and j are two network nodes, and the ratio of the maximum and minimum values is the network security ratio. In order to strengthen the real effect of cloud computing, this article calculates the Rand index of the network:

$$P = \frac{TP}{TP + FP} \tag{7}$$

$$R = \frac{TP}{TP + FN} \tag{8}$$

$$RI = P + R \tag{9}$$

$$RI' = RI + P + R \tag{10}$$

In formula (7–10), P is the accuracy rate; TP is the number of real nodes; FP is the number of false positive nodes; FN is the number of false negative examples; R is the recall rate; RI is the similarity measure of network nodes; RI' is the desired measure of network security.

3.3 Realize the Security Protection of the Network Boundary

In order to realize the security protection of the network boundary, this paper designs the above methods. The platform is composed of many sub-parts, and each part has its own specific function, and the combination of its functions. The platform has many elements, and each element is related to each other, showing a clear purpose, level, and being able to continuously adjust itself and adapt to the environment. Platform protection is a structured multidisciplinary approach used to define the concepts and requirements of complex and multi-faceted issues, including concepts, implementation and verification. Platform protection uses mathematics, physics and related scientific disciplines, as well as the principles and methods of protection design and analysis to formulate, predict and evaluate the vulnerability of the platform to security threats. The application fields of platform protection are very wide, including platform security in risky industries such as mining protection and tunnel protection. By combining multiple disciplines, analyzing and designing a platform suitable for the protection, the various parts of the platform can be optimized and controlled. The working principle of platform protection makes it have the characteristics of integration, integration and optimization. As an important object

of platform security protection, platform protection is essentially the use of a series of platform protection methods to assess whether the platform is safe, and organize suitable solutions for unsafe factors to avoid dangers, and minimize the hidden dangers in the platform. Specifically, the main purpose of platform security protection is to identify, minimize and control vulnerabilities and related risks. It is a multidisciplinary work that uses scientific principles, principles and methods to identify and assess vulnerabilities. Security analysis is the most important part of platform security protection. Only when security issues are analyzed comprehensively, correctly, and accurately, can we make feasible plans for security issues in the platform and avoid risks. For the analysis of platform security protection, different levels of analysis can be determined according to the needs of the project, including preliminary analysis, detailed analysis, etc. Analyze the existing security risks, and make scientific and reasonable predictions for each issue using platform security methods and principles.

4 Platform Test

In order to verify whether the platform designed in this article has practical effects, this article tests the above design. The test process and results are shown below.

4.1 Test Process

Connect the hardware and software of the platform to check whether there is a short circuit or short circuit. At this time, the hardware parameters of the protection platform are shown in Table 2.

Table 2. Hardware parameters

Parameter	Is it dangerous	Filter results
And	No	-
Exec	Yes	Success
Insert	Yes	Success
Select	Yes	Success
Delete	Yes	Success
Update	No	-
Count	No	-

As shown in Table 2, through the addition of different parameters, the degree of risk is relatively compared. The platform designed in this paper can filter the dangerous parameters, and the hardware operation effect is better at this time. After the hardware debugging is completed, this article debugs the software, and this article adds related cases, as shown in Table 3.

Table 3. Software test

Case study	Problem	Test effect
Physical security	Divide the area for management, set up standby power supply equipment in different areas, and the platform operation effect	Run successfully
Cyber security	Allow or deny the network access of portable and mobile devices according to the security policy. Terminate the network connection after the session is inactive for a certain period of time or after the session ends	The network is successfully connected or disconnected
Platform security	Use two or more combinations of authentication technologies for the same user to achieve user identity authentication; set sensitive marks for important information resources and all subjects who access important information resources	Mark the main resource successfully

As shown in Table 3, in terms of physical security, network security, platform security, etc. [15], the test results are all successful, indicating that the platform's software is operating normally. After the hardware and software are debugged, the login interface of the platform is shown in Fig. 2.

As shown in Fig. 2, after the hardware and software are debugged, the platform runs successfully at this time.

4.2 Test Results

In the above-mentioned test environment, this paper tests the performance of the two-way SM1 at the gateway boundary, and the test results are shown in Table 4.

As shown in Table 4, the performance results of two-way transmission of SM1 can be seen, the performance can reach 11.465 when the large packet of 1024 bytes is transmitted, the performance is only 1.109 when the small packet of 64 bytes is transmitted, and the performance is good when the large packet of 1518 bytes is transmitted. It reaches 9.031, so it can meet the encrypted transmission requirements of IoT gateways. Based on this, this paper tests the two-way SM4 at the gateway boundary, and the test results are shown in Table 5.

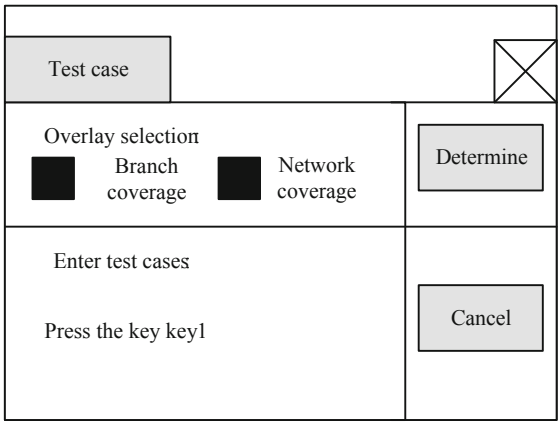

Fig. 2. Platform login interface

Table 4. Two-way SM1 performance test

Frame Size (bytes)	lntended Load (%)	Offered Load (%)	Throughput (R%)
64	1.109	1.109	3300.6
128	2.328	2.328	3932.5
256	5.984	5.984	5420.3
512	8.421	8.421	3957.3
1024	11.468	11.468	2746.2
1280	12.078	12.078	2322.7
1518	9.031	9.031	1468

Table 5. Two-way SM4 performance test

Frame Size (bytes)	lntended Load (%)	Offered Load (%)	Throughput (R%)
64	1.728	1.728	1.728
128	2.943	2.943	2.943
256	4.756	4.756	4.756
512	7.821	7.821	7.821
1024	11.486	11.486	11.486
1280	12.578	12.578	12.578
1518	8.412	8.412	8.412

As shown in Table 5, during the SM4 performance test, the lntended Load, Offered Load, Throughput and other indicators can be kept consistent. When the 1518 bytes large packet is transmitted, the performance is 8.412. At this time, the security effect of network data transmission better, therefore, can meet the security of the gateway boundary. Through the above test environment, the platform designed in this paper is compared with the traditional PB security protection platform and AP security protection platform. The test results are shown in Table 6.

Table 6. Comparison results of safety warning time of different methods

Number of experiments	Security warning time of traditional PB security protection platform/ms	Security warning time of traditional AP security protection platform/ms	The safety warning time of the safety protection platform designed in this paper/ms
1	0.11	0.15	0.01
2	0.23	0.24	0.03
3	0.26	0.31	0.04
4	0.28	0.36	0.05
5	0.30	0.42	0.05
6	0.31	0.44	0.05
7	0.35	0.46	0.05
8	0.36	0.48	0.05

As shown in Table 6, the security warning time of the traditional PB platform and AP platform is longer, both above 0.1ms, the response is slow, the protection effect is poor, and it does not meet the security protection requirements of the IoT gateway boundary. The platform designed in this paper has a shorter warning time, the longest warning time is 0.05ms, the response is faster, and the protection effect is better. It can meet the security protection requirements of the IoT gateway boundary and is of great promotion value.

5 Conclusion

With the continuous development of Internet technology and mature as well as the increase in Internet equipment, Internet of things has gradually spread to every aspect of People's Daily lives, and security is a big problem in the daily life can not be neglected. Therefore, many researchers gradually began to combine the Internet of things and security early warning theory, make full use of their respective advantages. It is widely used in transportation, industrial manufacturing, medical and health, disaster emergency

response and other fields. Therefore, an in-depth study of the security early warning system in the context of the Internet of Things is of great significance to all areas of people's daily production and life. The intelligent system, efficient management, and convenient monitoring it brings will also produce significant economic benefits. This article starts from the perspective of the security early warning system architecture of the Internet of things, based on the Internet of Things system architecture, first expounds and studies the three-layer network architecture of the perception layer, network layer and application layer, in order to meet the requirements of reducing delays and increasing transmission processing speeds. Improve the demand for system response, introduce cloud computing methods, and establish a cloud-side collaborative IoT security protection platform architecture, aiming to improve the security protection effect of the network and create conditions for the development of the Internet.

Fund Project. Science and Technology Project Number: GDKJXM20201931 [Research on Global Internet of Things Security Protection and Detection Technology].

References

1. Vajjha, H., Sushma, P.: Techniques and limitations in securing the log files to enhance network security and monitoring. Solid State Technol. **64**(2), 1–8 (2021)
2. Snehi, J., Bhandari, A., Snehi, M., et al.: Global intrusion detection environments and platform for anomaly-based intrusion detection systems. In: Proceedings of Second International Conference on Computing, Communications, and Cyber-Security. Springer, Singapore, pp. 817–831 (2021)
3. Zhao, S.: Simulation of scheduling fault tolerant control of big data cluster for security monitoring of cloud platform. Computer Simulation **38**(7), 486–490 (2021)
4. Sun, Q.Y., Liu, X.J., Sun, Y.M., et al.: A security wireless monitoring and automatic protection system for CCEL. Wirel. Commun. Mob. Comput. **2021**(1), 1–14 (2021)
5. Ma, H., He, J., Liu, Y., et al.: Security-driven placement and routing tools for electromagnetic side channel protection. IEEE Trans.on Computer-Aided Design Integrated Circuits Syst. **40**(6), 1077–1089 (2020)
6. Wang, C., Yu, L., Chang, H., et al.: Application research of file fingerprint identification detection based on a network security protection system. Wireless Commun. Mobile Comput. 1–14 (2020)
7. Zeng, R., Li, N., Zhou, X., et al.: Building a zero-trust security protection system in the environment of the power Internet of Things. In: 2021 2nd International Seminar on Artificial Intelligence, Networking and Information Technology (AINIT). IEEE, pp. 557-560 (2021).
8. Xuesong, H., Wei, L., Tao, Z., et al.: An endogenous security protection framework adapted to 5G MEC in power industry. In: 2021 China Automation Congress (CAC). IEEE, pp. 5155–5159 (2021)
9. Miki, T., Nagata, M., Sonoda, H., et al.: Si-backside protection circuits against physical security attacks on flip-chip devices. IEEE J. Solid-State Circuits **55**(10), 2747–2755 (2020)
10. Yen, C.C., Ghosal, D., Zhang, M., et al.: Security vulnerabilities and protection algorithms for backpressure-based traffic signal control at an isolated intersection. IEEE Trans. Intelligent Transportation Syst., 99, 1–12 (2021)
11. Liu, S., Liu, G., Zhou, H.: A robust parallel object tracking method for illumination variations. Mobile Networks and Appl. **24**(1), 5–17 (2018)

12. Xu, S., Qian, Y., Hu, R.Q.: Edge intelligence assisted gateway defense in cyber security. IEEE Network **34**(4), 14–19 (2020)
13. Robinson, T., Harkin, J., Shukla, P.: Hardware acceleration of genomics data analysis: challenges and opportunities. Bioinformatics **37**(13), 1785–1795 (2021)
14. Chen, B., Kim, H., Yim, S.I., et al.: Cybersecurity of wide area monitoring, protection and control systems for HVDC applications. IEEE Trans. Power Syst. **36**(1), 592–602 (2020)
15. Liu, S., He, T., Dai, J.: A survey of CRF algorithm based knowledge extraction of elementary mathematics in Chinese. Mobile Networks Appl. **26**(5), 1891–1903 (2021). https://doi.org/10.1007/s11036-020-01725-x