# Research on Security Access Technology of Power Internet of Things Gateway Equipment Based on Artificial Intelligence

Yanming Li[1](✉), Ying Fan[2], and Siyao Xu[2]

[1] Guangdong Power Grid Co., Ltd., Guangzhou 510030, China
lymflyingfish@163.com

[2] Electric Power Research Institute of Electrical Guangdong Power Grid Co., Ltd., Guangzhou 510080, China

**Abstract.** Aiming at the problem that the security access of traditional power Internet of things gateway equipment is vulnerable to network attack, resulting in the decline of security, a security access technology of power Internet of things gateway equipment based on artificial intelligence is proposed. Analyze the functional requirements of power Internet of things equipment, and carry out data protection processing of gateway equipment. Based on artificial intelligence technology, network attack characteristics are extracted to realize the secure access of power Internet of things gateway equipment. By means of comparative experiment, it is verified that the safety performance of the new technology is better and has great popularization value.

**Keywords:** Artificial intelligence · Power Internet of things · Gateway equipment · Secure access technology

## 1 Introduction

With the wide popularization of the Internet and the deepening of network applications, people have been used to using the services provided by the network to participate in various network activities, especially e-government and e-commerce [1]. Because the sensitive information stored and processed on the network is increasing day by day, network security management has become the primary problem to be solved in the computer network gateway equipment. Traditional network security management technologies include firewall, intrusion detection, security audit, network monitoring, security evaluation, authentication and authorization [2]. Reference [3] proposed a secure and universal wireless communication solution for the distribution Internet of things in smart grid. This paper mainly studies the secure ubiquitous wireless communication solution of distribution network Internet of things (pd_iot) in smart grid. The detailed topology of secure universal wireless communication network is given, and the integrated encryption and communication equipment is developed. The scheme supports a variety of state secret encryption algorithms, including SM1 / SM2 / SM3 / SM4 and forward

S.-H. Wang and Y.-D. Zhang (Eds.): ICMTEL 2022, LNICST 446, pp. 28–42, 2022.
https://doi.org/10.1007/978-3-031-18123-8_3

and reverse isolation functions, so as to realize PD_ Secure wireless communication of Internet of things services. With the emergence of new network mode, especially the emergence of distributed gateway devices, the traditional network security management methods gradually show the following shortcomings: at present, the commonly used authentication mechanisms are based on user identity, which is known, but in large-scale and open distributed gateway devices, users are not necessarily familiar with gateway devices.

The traditional security mechanism has no delegation mechanism, but in the distributed gateway device, the delegation mechanism can improve the flexibility of the gateway device and reduce the management workload of the gateway device. Traditional security mechanisms cannot handle new access conditions and restrictions, many security policy elements cannot be described directly, and their expressibility and scalability are poor [4]. There are multiple management domains in large-scale distributed gateway devices, and different management domains should adopt different security mechanisms, which can not enforce unified policy and trust relationship, while the current security mechanism can not manage domains. The traditional security mechanism makes the server fully realize access control, which increases the burden of the server, and the security is limited by the security of the server itself. Once the security of the server fails, the whole access control policy will not work [5].

In order to solve the above problems, trust management came into being. Trust management is a security management mechanism suitable for large-scale, open distributed gateway devices. Compared with the traditional security management mechanism, it has the characteristics of flexibility, reliability and scalability. Therefore, trust management is a new stage in the development of network security management. Intrusion detection and trust management play a “mainstay” role in network security management [6]. This paper studies the security access technology of power Internet of things gateway equipment based on artificial intelligence. By analyzing the functional requirements of power Internet of things equipment, the data protection processing of gateway equipment is carried out. Based on artificial intelligence technology, network attack characteristics are extracted to realize the safe access of power Internet of things gateway equipment. This method has more network throughput, can effectively shorten the response time and ensure better security performance.

## 2 Design of Secure Access Technology for Power Internet of Things Gateway Equipment Based on Artificial Intelligence

### 2.1 Analyze the Functional Requirements of Power IoT Devices

According to the objectives of network users, its production mode is mainly for multiple different factories distributed in different regions to jointly carry out the production process of products, which involves important links such as production commissioning and storage of products. These links have certain restrictions on the requirements of the on-site environment. Therefore, in the general control (regional headquarters) area, it is necessary to monitor the environment and production process, respond to emergencies for the first time, reduce unit losses, and ensure the safety of production products [4].

According to the goal of the network user unit [7], the network user unit has deployed different types of sensor acquisition equipment in the production workshop and warehouse (generally unattended workshop or warehouse) in its plant area, and deployed a gateway equipment that can collect relevant data and preprocess at a certain level in several areas (generally 3–5 production workshops or warehouse), after the gateway equipment is connected to the main network of the plant area and incorporated into the public network, the preprocessed data is transmitted to the regional headquarters. After the regional headquarters service network optimizes the data through its own algorithm and graphically processes it, it is presented to managers or leaders in a visual way for them to make early warning and decision-making in case of emergencies [8]. Therefore, network user units put forward special considerations on data security. Its overall framework is shown in Fig. 1.

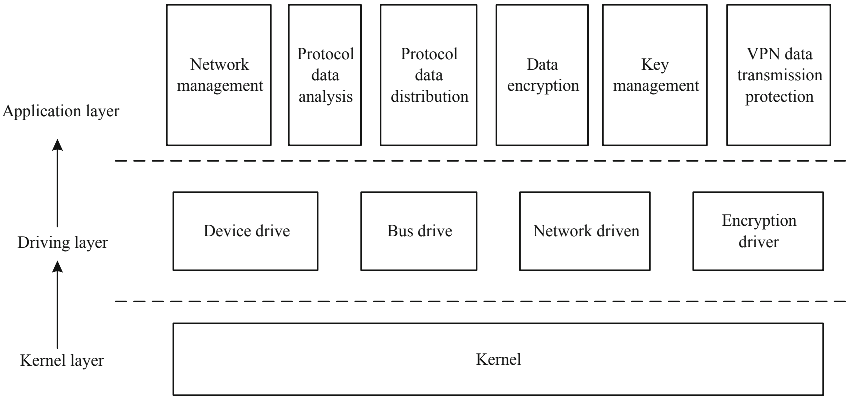

**Fig. 1.** Overall framework

As shown in Fig. 1, according to the overall framework diagram, the gateway device mainly completes the network kernel, data encryption and decryption, network management, and VPN data transmission protection. From the overall structure, in order to achieve network controllability and strong compatibility, the kernel still uses a tailored Linux kernel with a version of 3.18.17 [9]. The driver layer includes common devices, bus drivers and network drivers, which includes a variety of heterogeneous network protocol stacks to facilitate the analysis and distribution of protocol data. The encryption driver mainly provides a communication method (USB2.0) with the on-board hardware encryption chip (localized chip with encryption engine). When called by the application layer, the driver interacts with the hardware encryption chip to realize encryption and decryption. Function. The development of application layer adopts C + +, and the development of drive adopts C language.

According to the above description, it can be seen that the main functions of the gateway device include network management function, protocol data analysis and distribution, data encryption and decryption, key management and data transmission protection. At the same time, there are certain performance requirements for data encryption and decryption and data transmission protection [10]. Therefore, it is necessary to design the function first, complete the module corresponding to the function and the relationship between these function modules, and then design the corresponding business process in the follow-up. The device initialization module will initialize network parameters, load protocol types, and initialize various functional modules and interfaces according to the current network environment. The user obtains the corresponding network management authority through authentication login (USBKey + password), and adjusts and sets the network strategy of the device through a friendly interface. The network management module determines the mode of key generation, the configuration type of the VPN function, and the type of data filtering according to the strategy generated by the user [11]. When the externally collected data enters the device, it will first enter the data analysis and transceiver module, and then screen the data according to the packet filtering strategy set by the network management module. After that, the data will be sent to the data encryption and decryption module, while the VPN module obtains the network quintuple of the data and other information, and establishes a dedicated transmission channel in real time. When the data enters the encryption and decryption module, the module will generate and select the key according to the key management module, and perform encryption and decryption operations on the data. The encrypted and decrypted data is sent to the data analysis and transceiver module, and the module pushes the data to the destination according to the dedicated channel established by the VPN management module. After the entire transmission process is over, the VPN management module must remove the established dedicated transmission channel, the key management module will clear the key used for this transmission, and the network management module will clear the internal data cache without retaining any data information.

According to the division of functional modules and the relationship between modules, the software of the whole gateway equipment can be divided into several key processes. The whole gateway equipment software achieves the purpose of cooperative work through the interaction of these processes [12]. These key processes include equipment initialization, user authentication and login, authority control, firmware upgrade, factory setting recovery, key management, security policy management, protocol data analysis and distribution, data protection, status monitoring, etc. The design of each process will be described in detail below. The gateway device startup is mainly divided into two stages. The first stage is the bootloader startup and completes the inspection of the hardware interface or peripherals, such as wireless network interface, wired network interface, USB interface, hardware encryption and decryption chip, etc. [13]. Once it is found that the interface or peripherals cannot be started, the entire device initialization process will be stopped, and the fault indicator will be lit to remind the user or management personnel to repair. If the peripherals or interfaces are successfully started, the boot program will start the kernel and transfer the control of the device to the kernel. After the kernel obtains the disposal right, it will load the kernel modules, such as the algorithm interface module responsible for encryption and decryption, and the interface module for data transmission and reception and the gateway device management module responsible for management, etc., and automatically configure parameters for the startup of the services of these modules or processes, but when the module is found to be faulty and cannot be effectively started or configured, the kernel will stop the device start the initialization process, and light up the fault indicator to remind users or managers to repair the equipment.

The gateway device logs in to the device by providing wired Ethernet network and internal serial port. If you log in to the device from a wired Ethernet network, a web-based interface method is provided to log in. If you log in from the internal serial port, you will be provided with a printed character interface to log in. At the same time, the internal serial port is generally not open to the outside world and is mainly used by relevant technical personnel for production, debugging, and maintenance. The user logging in to the device is mainly to query, configure and audit the services of the gateway device. When you need to log in to the device, you need to first insert the USBKey into the USB-Host of the device and enter the password. If the device detects that the USBKey is not inserted, the user will not be able to log in to the device. The gateway device provides an SM2-based identity authentication method, so a password is required. The device uses the password as a factor to generate an SM2-based key pair, and performs two-way authentication of user identity together with the key pair pre-prepared in the Key. And return the authentication result. If the authentication result is wrong, it proves that the user password does not match the Key, and the user authentication login fails. If the authentication is successful, the key matches the user's identity. At this time, the device will read in the initialization information of the hidden area in the key, confirm the user's identity (management user, audit user, ordinary user), and assign permissions to it. In this way, the safety performance of the equipment can be initially guaranteed.

### 2.2 Perform Gateway Device Data Protection Processing

Data protection mainly provides a combination of privacy protection (password protection) and channel protection. First, the gateway device receives the collected data periodically reported by each node, and then classifies and preprocesses the data according to the strategy, and encapsulates the data according to the protocol (application protocol) negotiated with the management center, and transmits it after calling the transmission module. The transmission module will first consider encrypting the data after receiving the data, and establish a VPN transmission channel for this business, and report the encapsulated and encrypted data to the management center through the channel. After the service is completed, the VPN channel will be closed, and real-time connection to the VPN channel is not supported. After receiving the data, the management center obtains the actual node collection data through decryption, classifies it, and stores it in its database. When the collected data is abnormal, the management center will send an alarm to the administrator by means of short messages. After the device is started, it will automatically start a set of monitoring service processes, responsible for regularly collecting the running status of the gateway device, including the CPU running status of the device, the running status of the gateway device process, the network connection status, the packet filtering interception status, and the peripheral access status, the relevant information of whether the nodes under the gateway are operating normally or not, and report it to the management center, which is convenient for the management center to audit. In addition, in case of an emergency, such as abnormal network connection and the addition of an unauthorized authentication node, the gateway equipment will first send an alarm locally through audible and visual means. At the same time, it will report the alarm information to the management center according to the preset configuration strategy. After obtaining the alarm information, the management center will alarm the administrator through short messages. The external interface of the gateway device is shown in Fig. 2.

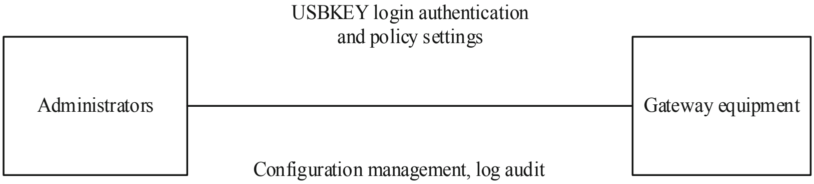
USBKEY login authentication
and policy settings
Administrators
Gateway equipment
Configuration management, log audit

**Fig. 2.** External interface of gateway equipment

As shown in Fig. 2, an external interface diagram is provided for the gateway device. The external interface of the gateway device is mainly for the administrator. The administrator needs to perform login authentication, policy setting, network configuration, log audit and other functions on the device. It mainly involves the management of gateway equipment. The device provides a unified login interface based on artificial intelligence. The functions mentioned in the above figure are integrated in the intelligent interface. The administrator needs to use the host to connect to the management network port and log in to the device through USBKey to carry out relevant management operations. Login authentication. After the administrator inserts the USBKey and enters the password according to the prompts, the interface is responsible for identity authentication and returns the authentication result. Policy settings. After logging in, the administrator enters the policy setting interface and configures relevant information on the interface, including firewall settings, IP packet filtering principles, supported IoT protocols, encryption methods, algorithms, etc. After that, the interface is responsible for generating configuration files and activating policies. Network settings. After the administrator logs in, enter the network setting interface. Configure device network parameters, including local address, node ID, background management center destination address, etc., and then the interface is responsible for generating configuration and activating. Log audit. This interface is responsible for collecting the policy execution status and network data filtering and forwarding alarm information of the local device for nearly a week, and presents it to the front-end interface after the administrator enters the log audit interface.

The internal interface mainly refers to the interface between the various modules inside the gateway device. The device is initialized. The first process executed after the gateway device is started needs to check the network configuration, whether the security policy configuration is normal, the service interface related to the gateway device, whether the main external hardware interface is normal, etc., and the device background service process will be started in order. Data reception. Data processing process call. The interface establishes two sets of threads. These two groups of sub-processes will receive data in two directions, one is from the management center to the gateway device, and the other is from the node to the gateway device, and respectively open up receiving resource pools for the data in the two directions, waiting for the data analysis and forwarding module to process. Data transmission. Data processing process call. The processed data is distributed in two directions. This interface establishes two groups of sending threads, and extracts data from the processed data sending queue and distributes it to the corresponding destination address. Intelligent management. The main process is called this interface. This interface is responsible for analyzing the administrator's configuration of the machine, including network configuration and security configuration, and after optimizing the configuration data, it is distributed to each execution module to complete activation. At the same time, this interface is also responsible for HTTPS service management. Key generation. The main process calls the interface. After the interface is called, it is responsible for interacting with the key management gateway device, and finally generates a key that can be used for encryption or authentication. SM2 certification. The gateway device management process is called. This interface is responsible for completing the integrity check of the received data and the two-way authentication of the user identity when the administrator logs in. Login authentication. The gateway device management process is called. After the administrator inserts the USBKey and enters the password according to the prompts, the interface is responsible for identity authentication and returns the authentication result. Protocol analysis. Data analysis and forwarding process call. This interface is responsible for the analysis and load stripping of the IoT protocol of the node.

Data confidentiality protection uses encryption algorithm to encrypt user data. Even if unauthorized users get the data, they can't know the content. The gateway equipment supports a variety of encryption algorithms in line with international standards, and also supports encryption algorithms independently developed and approved by the national competent department. At the same time, various encryption algorithms are implemented efficiently, which not only ensures the security of data, but also ensures the efficient processing of gateway equipment. In the design of gateway equipment, confidentiality protection is mainly applied in business data transmission protection, firmware upgrade, data packet transmission and so on. Integrity protection data is not modified by illegal users during transmission, or if a data packet transmitted on the network is modified by an illegal user, the receiver of the data can find that this is an illegally modified data packet. The non-repudiation of the data is used to prevent the user from refusing to acknowledge that a specific data packet has been sent. The processing method of this gateway device is to add a special message digest to the related IP datagram and encrypt the digest with a private key. After the data is transmitted to the destination, the corresponding public key is used to decrypt the digest, and the decrypted data is compared with the digest of the original data. If the comparison results are consistent, it can be determined that the data packet was sent by the user. The reason is that the encrypted private key is only held by the corresponding user, so it is effective to use this method to solve the non-repudiation of the data. The user specifies which network communication needs what kind of security protection. This is the VPN security strategy. The security policy selects data packets according to the source address, destination address, transport layer protocol, port, data transmission direction [14], etc. of the data packet, and encrypts, clears, and discards the selected data packet according to the needs of users. Security policy management is mainly embodied in the use of a central distribution mechanism based on the encryption and protection of configuration data in the gateway design, and the authority control mechanism used in the local configuration management of the gateway device. Through the above security protection mechanism, the access of the IoT gateway device is more securely protected.

### 2.3 Extracting Network Attack Characteristics Based on Artificial Intelligence

Artificial intelligence is a branch of computer science. It is a science that studies machine intelligence, that is, using artificial methods and technologies to develop intelligent machines or intelligent gateway devices to imitate, extend, and expand human intelligent behavior. Since the birth of the Dartmouth Conference in 1956, artificial intelligence has made gratifying progress on bumpy roads, especially in machine learning, data mining, computer vision, expert gateway equipment, natural language processing, pattern recognition and robotics and other fields. In order to extract the characteristics of network attacks more truthfully, this paper conducts an intelligent analysis on them as follows.

$$\mu_{X_i}(x_l) = \mu_{il} = \begin{cases} 1, x_l \in X_i \\ 0, x_l \notin X_i \end{cases} \tag{1}$$

$$M_h = \{\mu_{il} | \mu_{il} \in \{0, 1\}\tag{2}$$

$$M_f = \left\{ \mu_{il} | \mu_{il} \in \{0, 1\}, \sum_{j=1}^{k} \mu_{il} = 1 \right\} \tag{3}$$

$$\hat{M_f} = \frac{M_h}{\sqrt{\mu_{X_i}(x_l)}} \tag{4}$$

In formula (1–4), $\mu_{X_i}(x_l)$ is the network sample subset; $\mu_{il}$ is the function set of the network sample; $x_l$ is the membership function; $X_i$ is the feature vector; $M_h$ is the unit function; $M_f$ is the unit basis vector; $\hat{M_f}$ is the normalization the unit basis vector to be processed. From that we get:

$$D = (x_l - p_i)^T (x_l - p_i) \tag{5}$$

$$(x_l - p_i) = \frac{(x_l - p_i)^T (x_l - p_i)}{D^2} \tag{6}$$

$$C = \sum_{i=1}^{k} D \tag{7}$$

$$U = \sum_{i=1}^{k} \mu_{il}^{m} \tag{8}$$

$$D(x_l - p_i) = \sum_{i=1}^{k} \sum_{l=1}^{n} U \tag{9}$$

$$P^* = \{p_i | 1 \le i \le k\} \tag{10}$$

In Eq. (5–10), $D$ is the dissimilarity measure; $p_i$ is the optimal intelligent analysis effect; $T$, $m$, $n$ and $k$ are constants; $C$ is the objective function of network attack; $U$ is the optimal intelligent analysis prototype; $D(x_l - p_i)$ is distortion; $P^*$ is a fuzzy function.

This technology is mainly aimed at the processing of gateway equipment after upgrade failure. After the upgrade fails, the most ideal state is to monitor the startup process when the gateway device boots, and automatically select whether the fallback version is required through the state judgment. The key technical point is how to supervise the whole startup process, because the control of CPU will be transferred and the life cycle of boot software will end. By establishing the start state base in an address segment of the memory, the automatic fallback of the version can be realized to a certain extent. After the boot software is started, read the status base recorded in the previous startup process to judge whether version fallback is required. In addition, the timing of rollback is very important. The following situations need to be considered, which may cause misoperation in the version rollback process. During equipment startup, the hardware is powered off. This situation will make the state base unable to update, triggering version fallback. When there is no ups (standby power supply), the CPU hardware register cannot record any status or fill in the status base after power failure. After repowering up, it is difficult to judge whether the startup failure is due to hardware power failure or upgrade failure. After power on again, the boot software will still perform version fallback, resulting in misoperation. The upgraded file is incorrect, but it will not affect the basic operation of the operation gateway device. After the upgrade, the configuration of the software has problems, which will affect the business operation, but will not affect the normal startup and operation of the operation gateway equipment. Such errors will not cause the software to report errors or exit abnormally, and it is difficult for the boot software or kernel to be notified. Finally, the temporal and spatial randomness of such errors is strong, so it is difficult to monitor them by fixed inspection methods. Therefore, the boot software will not judge such errors as upgrade failure, and will continue to load the software gateway device with business problems. To sum up, the determination of the fallback time of gateway equipment is a complex and comprehensive determination process. At present, there is no very perfect fully automatic fallback scheme in the field of operating gateway equipment.

Based on artificial intelligence, this paper extracts the characteristics of network attack, which can maximize the security access effect of gateway equipment and ensure the normal operation of equipment.

### 2.4 Realize the Secure Access of Power IoT Gateway Equipment

After completing the detailed design of the Internet of things gateway software, the corresponding verification and testing work is carried out on the gateway equipment to verify whether the gateway equipment meets the needs of practical application. The verification and test work is carried out in the corresponding test environment built by using the actually developed gateway equipment. The purpose of the test is to verify the compliance of the gateway equipment with the requirements in the actual application scenario and whether it meets the design security. The testing work includes two parts: verification of management and business functions and verification and testing of security. The first part of the function verification work is as follows: the verification of the gateway device management function and service function, such as device initialization, user login, authority control, firmware upgrade, verifies the function design and interface design of the gateway software; The verification of protocol data analysis and distribution function verifies the basic business functions of Internet of things gateway equipment. The second part of the test work is as follows: the national secret algorithm encryption and decryption function verification, encryption and decryption performance test, key management function verification and data transmission protection function verification of the gateway equipment. Verify whether the actual gateway equipment meets the expected security design requirements. This paper will introduce the environment, process and conclusion of verification and testing in detail.

The administrator opens the management interface, enters the device IP address, and the gateway device checks whether the device has been initialized, prompts the user and starts the initialization operation. Select the standard that the device follows and execute the next step. The gateway device prompts the user to confirm the standard. Choose the authentication method of the administrator: if the administrator chooses to use the key authentication, check whether the user inserts the USBKey, otherwise prompt the user to insert the USBKey; then enter the PIN code of the USBKey; verify the correctness of the PIN code, the wrong PIN code prompts the user, when the number of PIN code errors exceeds 5 times, the USBKey is locked, the gateway device verifies the validity of the USBKey, and the illegal key refuses to generate a certificate request and prompts the user; the gateway device administrator, security administrator, and security auditor are initialized in turn. The gateway device prompts that the initialization is complete and records the log, and enters the login interface.

The administrator enters the gateway device login interface. Enter the administrator name, password, verification code or USBKey + PIN. The gateway device verifies the legitimacy of the administrator. An illegal user refuses the next operation and prompts the user. If the number of consecutive incorrect password entries exceeds the set threshold, the user will be locked. The gateway device needs to convert the IoT protocol of the perception layer into a standard Ethernet frame and send it to the application layer service gateway device. The standard command issued by the service gateway device can be converted into the IoT protocol format and forwarded to the perception layer node. The verification of this function is mainly done with the help of a user protocol analyzer. According to the above method, the secure access of the gateway device is realized.

## 3 Experiment and Analysis

In order to verify whether the technology designed in this article has the effect of use, this article conducts experiments on the above methods. The experimental process and results are shown below.

### 3.1 Experimental Process

This experiment first collects network node data, and then uses the method designed in this article for data processing, and applies the obtained data to the experiment. At this time, the internal interface of the gateway device is shown in Table 1.

**Table 1.** Internal interface description

| Interface | Name | Describe |
|---|---|---|
| wst_dev_init() | Device initialization | The first process executed after startup needs to check the network configuration, whether the security policy configuration is normal, the service interface related to the gateway device, whether the external main hardware interface is normal, etc. and the device background service process will be started in order |
| wst_data_receive() | Data reception | Data processing process call. The interface establishes two sets of threads. These two groups of sub-processes will receive data in two directions, one is from the management center to the gateway device, and the other is from the node to the gateway device, and respectively open up receiving resource pools for the data in the two directions, waiting for the data analysis and forwarding module to process |
| wst_data_send() | Data sending | Data processing process call. The processed data is distributed in two directions. The interface establishes two groups of sending threads, and extracts data from the processed data sending queue, and distributes it to the corresponding destination address |
| wst_sm4_verify() | VPN management | Data analysis and forwarding process call. Before sending data, a VPN tunnel needs to be established. This interface is responsible for establishing the tunnel and closing the tunnel after the service is completed |

As shown in Table 1, data confidentiality protection uses encryption algorithms to encrypt user data, even if unauthorized users get the data, they cannot know the content. The gateway equipment supports a variety of network encryption effects that comply with international standards, and also supports self-developed encryption algorithms approved by the national competent authority. At the same time, various network encryptions are also efficiently implemented, which not only guarantees the security of data, but also guarantees the efficient processing of the system. At this time, the resource configuration of the gateway device is shown in Table 2.

As shown in Table 2, for the resource configuration of the gateway device, because the role of the Internet of Things gateway is to connect the perception layer network and the Internet network as an intermediary, it must adapt to various perception layer network protocols, convert data between different protocols, and quickly connect enter the Internet network to control and manage various sensors. Therefore, under this configuration condition, the security of the gateway device can be guaranteed.

**Table 2.** Gateway device resource configuration

| Resources name | Quantity | Model |
|---|---|---|
| IoT gateway | 2 | Operating System: Linux<br>Network port: 5, of which 4 are switching ports |
| Switch | 1 | Huawei Quidway S5700 |
| Network tester | 1 | Spirent Test Center 9000 |
| Test PC | 2 | Pentium(R)Dual-CoreE5300/2 g/500G<br>Windows XP, IE8 |

### 3.2 Experimental Results and Discussion

Under the above experimental environment, the network security access technology designed in this paper is tested. The network security access can be detected by the network packet loss rate and response time. Therefore, this paper tests the above two indicators, and the test results are shown in Table 3.

**Table 3.** Test results of throughput

| Throughput(Mbps) | Reference [3] technical network throughput | Technical network throughput designed in this paper |
|---|---|---|
| No package | 93.976 | 98.961 |
| Pause time between two private rooms 10 ms | 93.732 | 99.895 |
| Pause time between two private rooms 1 ms | 93.601 | 99.253 |
| Full speed contracting | 32.536 | 18.426 |

The meanings of the four evaluation indicators in Table 3 are, respectively, the throughput when no packets are sent, the throughput when the pause is 10 ms, the throughput when the pause is 1 ms, and the throughput when the packets are sent at full speed. As shown in Table 3, through the four test environments of No package, 10ms pause time between two packets, 1ms pause time between two packets, and Full speed contracting, the reference [3] technology has less network throughput, below 94.0, when Full speed contracting, the throughput is 32.536, the throughput effect is poor, and it does not meet the security requirements of gateway equipment; Under the same conditions, the technology designed in this article has a large network throughput, above 98.0, when Full speed contracting, the throughput is 18.426, and the throughput is better, which meets the security requirements of gateway equipment. In addition, this article tests the security response time of the network, and the test results are shown in Table 4.

As shown in Table 4, in the four test environments of No package, 10ms pause time between two packets, 1ms pause time between two packets, and Full speed contracting,

**Table 4.** Test results of response time

| Response time (s) | Reference [3] technology network security response time/s | This paper designs the technical network security response time/s |
|---|---|---|
| No package | 0.851 | 0.085 |
| Pause time between two private rooms 10 ms | 0.854 | 0.085 |
| Pause time between two private rooms 1 ms | 0.855 | 0.085 |
| Full speed contracting | 2.459 | 0.814 |

the reference [3] technology network security response time is longer. Above 0.8 s, Full speed contracting. When the network security response time is 2.459, the network security effect is not good; Under the same conditions, the technology designed in this paper has a short network security response time. Within 0.1s, when Full speed contracting, the network security response time is 0.814, and the network security effect is better. Through the above test, this paper compares the number of attacks on the reference [3] technology gateway device network with the number of attacks on the technology gateway device network designed in this paper. The experimental results are shown in Table 5.

**Table 5.** Experimental results

| The amount of data | The number of attacks/times of the reference [3] technology gateway device network | The number of attacks/times of the technical gateway device network designed in this article |
|---|---|---|
| 1000 | 248 | 24 |
| 2000 | 556 | 35 |
| 3000 | 827 | 42 |
| 4000 | 1516 | 51 |
| 5000 | 1612 | 95 |
| 6000 | 2745 | 106 |
| 7000 | 3871 | 132 |
| 8000 | 4987 | 163 |

As shown in Table 5, under the same experimental environment, this article conducted 8 experiments, and obtained the reference [3] technology gateway equipment under the conditions of the data volume of 1000, 2000, 3000, 4000, 5000, 6000, 7000, and 8000. The network has been attacked more frequently. As the amount of data increases, the number of attacks will also increase, and the network security performance is poor; and under the same conditions, the technical gateway device designed in this article has fewer attacks on the network, and the network is safe. High performance. This meets the research purpose of this article.

## 4 Conclusion

This paper studies the security access technology of power Internet of things gateway equipment based on artificial intelligence. By analyzing the functional requirements of power Internet of things equipment, the data protection processing of gateway equipment is carried out, so as to effectively ensure the security of network being attacked. Based on artificial intelligence technology, network attack characteristics are extracted to realize the safe access of power Internet of things gateway equipment. This method has more network throughput and shorter network security response time. This article analyzes the structure of the gateway. The role of the Internet of Things gateway is to connect the perception layer network and the Internet network as an intermediary. It must adapt to various perception layer network protocols, convert data between different protocols, and quickly access the Internet network. Sensors for control and management. In order to ensure the integrity of the gateway device of the Internet of Things, it can also provide various peripheral interfaces for different types of devices. The dynamic loading module is used to ensure that the software module can be dynamically loaded under different environmental requirements. It is applied in actual scenarios, so that the IoT gateway device has the characteristics of flexibility, generality, and scalability. At the same time, the gateway studied in this paper uses hardware encryption technology and VPN technology to protect the data and improve the integrity and reliability of the data.

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

## References

1. Zhan, K.: Design of computer network security defense system based on artificial intelligence and neural network. J. Intelligent and Fuzzy Syst. **9**, 1–13 (2021)
2. Chu, M., Song, Y.: Analysis of network security and privacy security based on AI in IOT environment. In: 2021 IEEE 4th International Conference on Information Systems and Computer Aided Education (ICISCAE). IEEE, 390–393 (2021)
3. Chen, L., Suo, S., Kuang, X., et al.: Secure ubiquitous wireless communication solution for power distribution internet of things in smart grid. In: 2021 IEEE International Conference on Consumer Electronics and Computer Engineering (ICCECE). IEEE, 780–784 (2021)
4. Kou, G., Wang, S., Tang, G.: Research on key technologies of network security situational awareness for attack tracking prediction. Chin. J. Electron. **28**(01), 166–175 (2019)

5. Chemouil, P., Hui, P., Kellerer, W., et al.: Special issue on artificial intelligence and machine learning for networking and communications. IEEE J. Selected Areas in Communications **37**(6), 1185–1191 (2019)
6. Padmaja, M., Shitharth, S., Prasuna, K., et al.: Grow of artificial intelligence to challenge security in IoT application. Wireless Personal Communications, pp. 1–17 (2021)
7. Liu, S., Liu, G., Zhou, H.: A robust parallel object tracking method for illumination variations. Mobile Networks Appl. **24**(1), 5–17 (2018)
8. Li, G.: DeSVig: decentralized swift vigilance against adversarial attacks in industrial artificial intelligence systems. IEEE Trans. Industrial Informatics **16**(5), 3267–327 (2019)
9. Zhou, C., Liu, Q., Zeng, R.: Novel defense schemes for artificial intelligence deployed in edge computing environment. Wirel. Commun. Mob. Comput. **2020**(8), 1–20 (2020)
10. Sikora, P., Malina, L., Kiac, M., et al.: Artificial intelligence-based surveillance system for railway crossing traffic. IEEE Sensors J. **21**(14), 15515–15526 (2020)
11. Zhang, Z., Yang, Y.: Design of remote monitoring system for a mechanical equipment based on internet of things. In: 2021 7th Annual International Conference on Network and Information Systems for Computers (ICNISC). IEEE, pp. 54–59 (2021)
12. Foubert, B., Mitton, N.: Lightweight network interface selection for reliable communications in multi-technologies wireless sensor networks. In: 2021 17th International Conference on the Design of Reliable Communication Networks (DRCN). IEEE, pp. 1–6 (2021)
13. Namasudra, S., Chakraborty, R., Kadry, S., et al.: FAST: fast accessing scheme for data transmission in cloud computing. Peer-to-Peer Networking Appl. **14**(4), 2430–2442 (2021)
14. Zhang, J., Hou, X.: Simulation of layered filtering method for multi-channel false data in sensor networks. Computer Simulation **37**(02), 339–342,364 (2020)