International Journal of Latest Research in Engineering and Technology (IJLRET)
ISSN: 2454-5031
www.ijlret.com || Volume 05 - Issue 12 || December 2019 || PP. 16-23

Design and Implementation of Power Security Gateway Based on SSL VPN Technology

He Hui[1*], Zhao Tianrui[1]
[1](*School of Control and Computer Engineering, North China Electric Power University, Beijing 102206, China)*

Abstract: In order to improve the operation efficiency of electric power enterprises, improve staff flexibility and office quality, realize the safe access of mobile terminals to the intranet of electric power enterprises, and avoid interception, tampering and destruction of interactive information, this paper designs and implements a power security gateway based on SSL VPN technology according to the characteristics and requirements of information security construction in the electric power industry. The gateway is designed according to the national security standard. It can protect the interactive information by establishing a secure channel and controlling the access of users. At the same time, it can also authenticate the identity of the mobile terminal to ensure the safety and reliability of the terminal. It has certain practical significance for the information transmission and internal resource security protection of power enterprises.

Keywords: Electric Power Enterprise, Secure Access, Security Gateway, SSL VPN

I. INTRODUCTION

With the rapid construction of smart grid and the rapid development of mobile communication technology, more and more different types of mobile terminals are connected to the power enterprise intranet by different access methods. At the same time, different services of power enterprises are also expanding to mobile terminals.The mobile terminals connected to the intranet of electric power enterprises mainly have the characteristics of various types, large quantity, high requirements for data security and real-time performance, wide coverage, etc.In addition, the internal network of electric power enterprises has its own application system partition, classification, domain division, and internal and external network isolation, which also brings difficulties to the exchange of data and information.How to realize the safe access of mobile terminals, expand the accuracy and real-time of data exchange, and realize the considerable and controllable process of power production and operation is a problem to be solved by power enterprises at present [1].

SSL VPN is a proxy technology that does not require users to connect to the corporate server to access internal corporate resources. At present, SSL VPN is the most simple, effective and secure solution for remote users to access sensitive corporate data. As an emerging remote secure access method, it is widely used [2-3]. Literature [4] aimed at the problem that the common security access equipment in the power industry could not meet the needs of users, and proposed an SSL VPN-based application software hardening solution, which improved the office efficiency of employees, reduced data security risks, and guaranteed the stability of power grid business. Literature [5] researched and improved the working principle of SSL VPN. After the improvement, it can provide support for weaker network border security protection. Literature [6] analyzed the defects of VPN, and then proposed an isolated gateway architecture, which has certain positive significance for deepening the understanding of VPN security. Literature [7] designed and implemented a secure socket protocol based on Android system for the transmission of user sensitive information. The protocol uses national secret algorithm, which effectively improves the security of the system on the premise of meeting the functional requirements of users.

Based on the information security requirements of the power industry, this paper uses SSL VPN proxy technology to design and implement a secure gateway for power companies. The security gateway adopts Dingxin security chip and is designed in accordance with the national secret SSL VPN standard specifications. It is mainly responsible for establishing a secure channel and controlling access to users, encrypting transmitted data to prevent interception, tampering and destruction. At the same time, the identity information of the mobile terminal can be authenticated to ensure that the terminal is trusted. This has certain practical significance for the power company's information transmission and the security protection of internal resources.

II. DESIGN PRINCIPLES

A. Security Principle

VPN is a virtual network built in an open Internet network environment. All network information interaction is carried out in the Internet network environment. However, for electric power enterprises, these data and information are private and cannot be acquired by irrelevant personnel outside the enterprise.In addition, users using VPN should be authorized users, and unauthorized users are prohibited from logging into

VNP network.In order to ensure the security of VPN network, the user's identity can be identified, and the user's access terminal and access authority can be identified to prevent illegal users and illegal terminals from accessing, thus causing potential safety hazards to the power enterprise system [8-9].

B. High-Speed Principle

The biggest limitation of remote access is the speed of network transmission. Slow access speed will greatly reduce the office efficiency of employees. The reasons for the slow network transmission speed may be multiple reasons such as transmission data redundancy, high packet loss rate and delay of network data packets, and wireless access by mobile devices. Through the analysis of these reasons, it can be optimized and upgraded from the four levels of line, transmission protocol, data and application, thereby solving the problem of timeliness.

C. Usability Principle

For users, how to use VPN network simply and efficiently is the key point.However, the current general knowledge reserve of end users is insufficient, and further study is needed for the use of communication equipment. The biggest purpose of using VPN network is to access the internal network of the headquarters for remote office. This requires simplifying the operation as much as possible, reducing the difficulty, avoiding complicated client configuration operation, and improving the office efficiency of users to the greatest extent.On the other hand, it can also greatly reduce the workload of network managers in maintaining VPN clients.

D. Stability Principle

Access to the internal resources of power companies by power companies needs to rely on the VPN network, so the VPN network is an important support for the remote access of the entire network of the enterprise. Once a failure occurs due to some reasons, it will not only affect the corporate office, but also cause serious network accidents and bring significant losses [10]. Therefore, the efficient and stable operation of VPN is very important. It is necessary to consider not only network issues but also power business issues.

III. OVERALL ARCHITECTURE

The security gateway uses thread pool technology and high-speed network framework to improve the utilization rate of computer resources, so that the CPU and I/O equipment of the computer can be fully utilized to ensure the concurrent access of mobile terminals.Secondly, the security gateway uses SM2 digital certificate and other authentication methods (user name/verification code, etc.) to realize multi-factor identity authentication of mobile terminals, and uses the national security standard SSL communication protocol to realize secure data transmission. the overall architecture of the security gateway is shown in Fig. 1.

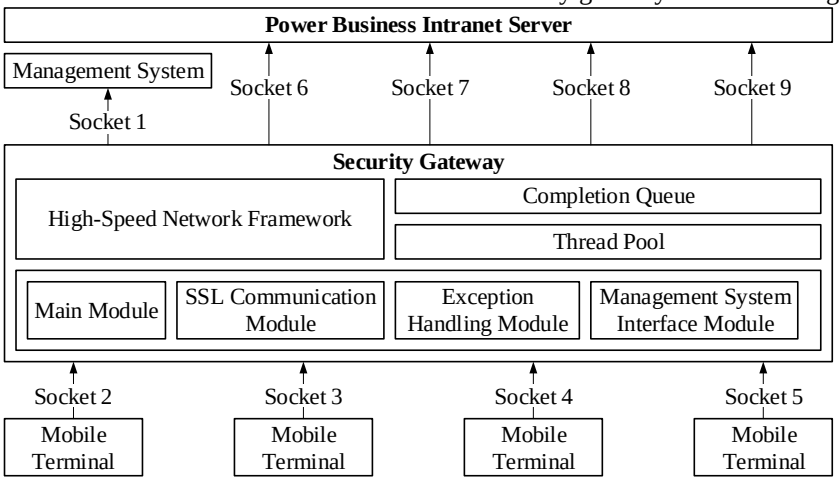

figure 1. SSL VPN security gateway architecture

The security gateway is located between the mobile terminal and the power service intranet server and needs to process the data of both parties simultaneously.Every time the security gateway receives data, it will first judge the type of data message. The key agreement message and ciphertext message are processed in different ways.In the process of data transmission, the data can reach the intranet server through the security gateway by the mobile terminal, or the intranet server can reach the mobile terminal through the security gateway.The former's data interaction process is based on the secure channel, while the latter's data interaction

process is based on the former's data interaction process. Therefore, the mobile terminal must first complete the key negotiation based on the national secret SSL protocol with the security gateway. The security gateway will only establish the communication connection with the intranet server if the key negotiation passes.On the contrary, if the key agreement fails, the security gateway's exception handling module will return the error code and close the connection at the same time. After the key agreement is completed, the security gateway will process the data sent by the transfer terminal and then send it to the intranet server. in case of data sending or receiving errors, the security gateway will also send an error code to the mobile terminal and close the connection at the same time. the operation flow of the security gateway is shown in Fig. 2.

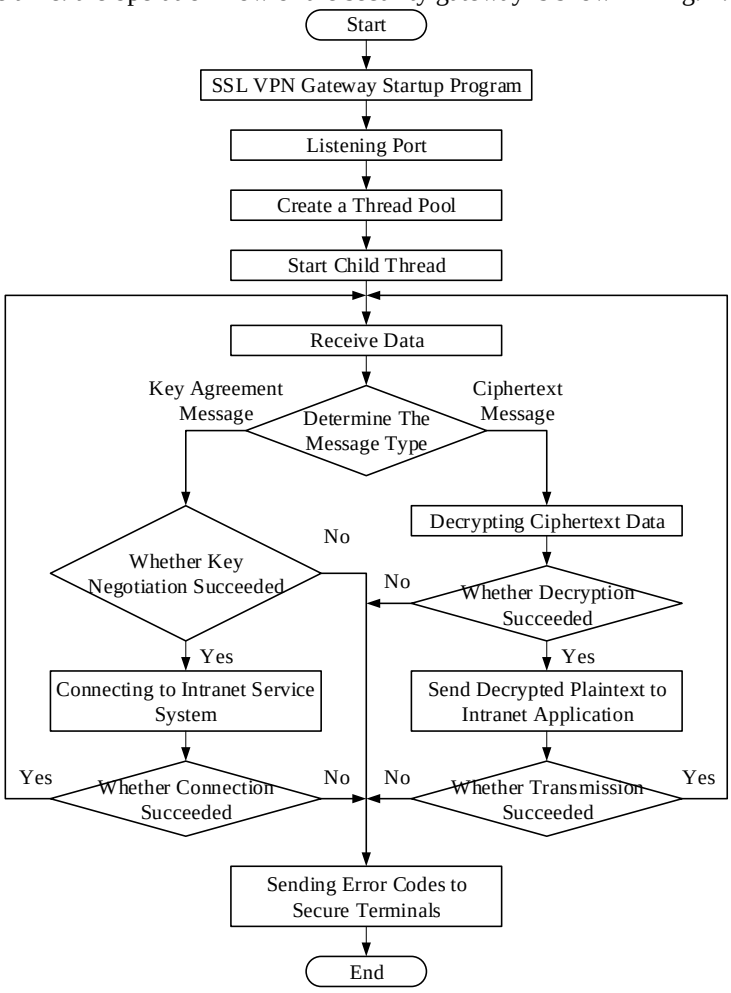

figure 2. mobile terminal security access flow chart

In order to ensure the legality and credibility of user access, the security gateway must support not only user account password authentication, but also digital certificate authentication, mobile USB KEY authentication, and other hardware authentication methods. This not only improves the security of the security gateway, but also allows the power company to combine client authentication methods according to the corresponding security level when selecting, ensuring the security of the internal network resources of the power company to the greatest extent.

At the same time, in order to prevent users from leaving for a long time without logging off, others can peep into the confidential information inside the security gateway, and an inactivity detection engine is also added to the security gateway.

When the security gateway detects that the user is no longer active, a prompt box will pop up asking the user "The SSL communication connection will disconnect after a timeout in N seconds. Do you continue to use it?" If the user remains active in time, the communication will not be active Disconnected [11]. If the user fails to remain active within the specified time to perform the operation within the time limit, the security gateway will determine that the user has timed out, automatically disconnected from the intranet server, and logged out of the local user account to log in and return to the login interface.

After logging in to the security gateway, the mobile terminal user will form a virtual private line with the internal service server system. At this time, the user can no longer access network resources outside the virtual private line. The purpose of this is firstly that after users enable the virtual private line function, insecure factors in the external network can no longer pose a threat to the VPN system. Secondly, it is also possible to avoid the possibility of information leakage caused by insecure factors on the client and avoid hidden security risks caused by the mobile client, thereby ensuring the security of the internal server of the power company.

IV. IMPLEMENTATION PLAN

A. Main Technology

1) Thread Pool Technology

The thread pool technology creates a group of sub-threads in the thread when the server starts up, and puts these sub-threads into the thread queue and is in a sleep state.When the system has new tasks to allocate, the main thread will select the threads in the thread pool through a preset selection algorithm, such as random algorithm, rotation selection algorithm and shared queue algorithm.When the sub-thread is selected, the main thread also needs to notify the target sub-thread that a new task arrives and needs to be processed, and transmit the corresponding data in the past. Channels or global variables can be used to realize information interaction between threads.The information interaction model of thread pool is shown in Fig. 3.

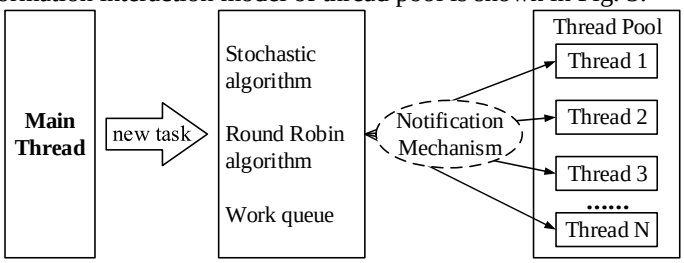

figure 3. thread pool information interaction model

Thread pool technology is mainly applied to applications with shorter time and higher performance requirements. That is, thread pool technology is suitable for applications with high concurrency in a short time. It can not only make full use of system resources, but also improve the performance of servers and the utilization rate of system resources [12].

2) User Mode Protocol Stack Technology

Most traditional VPN products based on the TCP/IP protocol network architecture consume most of the system resources for processing TCP/IP requests and HTTP protocol parsing. As the number of concurrent users increases, the performance of the system will drop dramatically. The security gateway uses the high-speed protocol stack technology to integrate the TCP/IP protocol suite into one, thereby reducing calls between protocols and achieving the purpose of streamlining high speed.

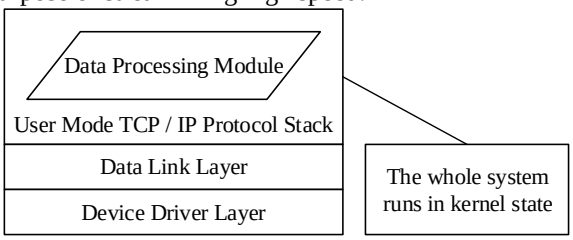

figure 4. logic architecture of high-speed protocol stack

High-speed protocol stack technology eliminates the performance loss of CPU switching between user state and kernel state frequently, and the whole system always runs in kernel state.In addition, the high-speed protocol stack only obtains the data to be processed from the data link layer and discards other irrelevant data, which further saves system resources and optimizes system performance [13].

3) Connection Multiplexing Technology

In a typical network topology, the security gateway is located between the mobile terminal and the power service intranet server.In this case, the security gateway acts as a middleman. If the user requests to meet the security requirements, the security gateway will forward the request to the intranet server, forming a one-to-one relationship.This will not cause problems when the network traffic is small.However, when the network

traffic increases sharply, the intranet server is usually unable to handle many highly concurrent connections, as shown in Fig. 5.

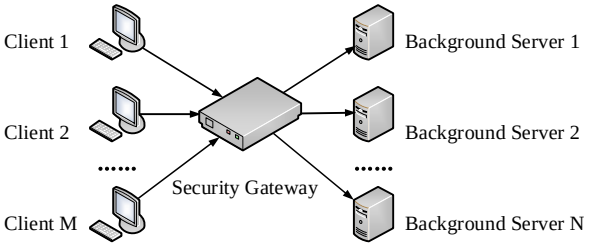

figure 5. background connections for typical network topology

On the other hand, each connection in the intranet server needs to occupy certain system resources to save connection information.Therefore, when the number of users increases sharply, the intranet server will soon be unable to continue service due to the exhaustion of system resources. However, this does not mean that the network does not have enough bandwidth and the server does not have enough throughput and processing capabilities.This shows that the TCP/IP protocol stack of the intranet service server cannot adapt to many connection requests, thus causing the intranet server to crash and unable to continue to provide services.In addition, many applications may use many short connections, which will also lead to the exhaustion of intranet server system resources.

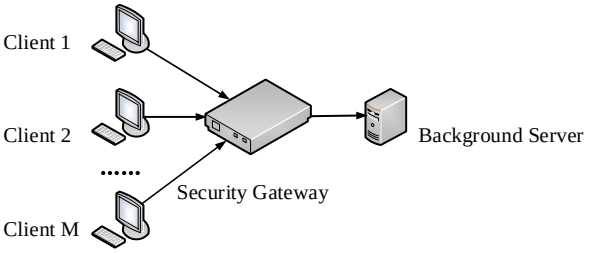

figure 6. background connection using connection multiplexing technology

As shown in Fig. 6, the security gateway establishes a plurality of connections with the background server in advance by using the connection multiplexing technology. user requests will be distributed according to the load balancing algorithm, and then the security gateway will select a connection in the connection pool established first by using the selection algorithm and send user requests through the connection. this not only makes full use of the throughput capacity of the server, but also can reduce the pressure of the intranet server and improve the overall operation efficiency of the internal system of the enterprise [14].

4) Multi-Virtual IP Pool Technology

IP Tunnel technology can perfectly support all data transmission above IP layer.For users to better use IP resources, IP Tunnel must obtain the corresponding virtual IP before it can work properly.However, for large power group companies, IP has been planned, and identity binding needs to be implemented according to IP accessed remotely. Fixed virtual IP can be bound for each user, thus realizing the binding of user identity and virtual IP.If there are not so strict requirements for user access, but various departments within the group have already planned IP segments, in order to distinguish different departments through IP segments, user groups can be bound with IP pools.For users authenticated by a third party, they can read the virtual IP information on LDAP (Lightweight Directory Access Protocol) and RADIUS server, thus realizing perfect combination with the third party.

B. Terminal Security Access Scheme

In order to ensure the security of information transmission, the secure access of mobile terminals is also extremely important.Using mobile terminals for extensive access, the office efficiency and flexibility of enterprise employees have been improved, and the operation efficiency of enterprises has also been improved.However, for the power industry, palmtop computers and smart phones have many remote accesses. Although identity authentication, encryption of private data, SIM card binding and log recording are used to ensure the security of access terminals to some extent, the IMSI attached to the SIM card, that is, the

international mobile subscriber identity number, can be forged. In case of forgery, the application system in the power enterprise intranet will face security risks.

In addition to the above problems, mobile terminals also face the risk of losing malicious software and equipment.Therefore, it is extremely important to improve the reliability and credibility of mobile terminal authentication and standardize the user's operation behavior [15].

As shown in Fig. 7, in order to establish a unified connection between enterprise mobile devices and VPN security gateways in different operating systems, a unified mobile application access security gateway scheme is proposed.Mobile access terminals are mainly divided into Android, IOS mobile phone terminals and Android operation terminals. SSL communication is used with the security gateway and RSA/SM2 encryption algorithm is used for encryption.The certificate system is responsible for the identity authentication of the mobile terminal access, and mainly carries out identity authentication through RSA/SM2 KEY certificates such as secure TFCard and Bluetooth Key to ensure the security and feasibility of the mobile terminal access.

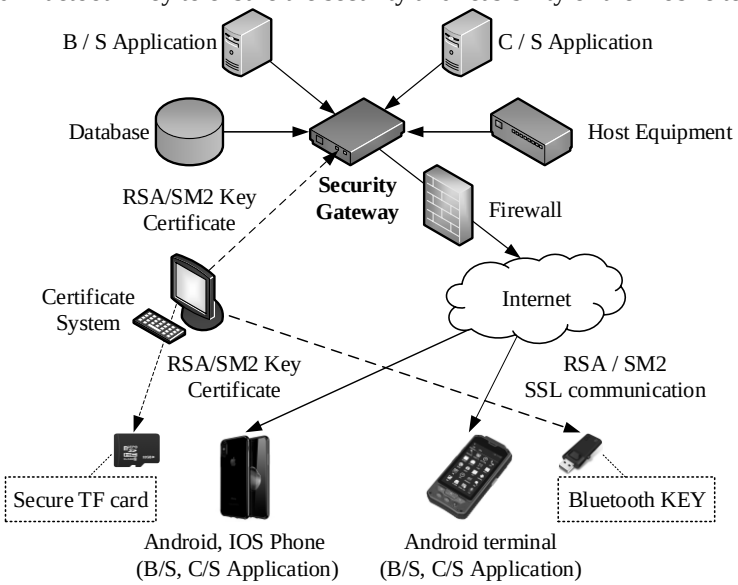

figure 7. mobile terminal security access scheme

The mobile terminal establishes communication connection with SSL VPN through SSL channel, which mainly includes three modules: security check, network access authentication and security communication. The security communication includes data encryption, identity authentication and security chip.The specific safety protection schematic diagram is shown in Fig. 8 [16].

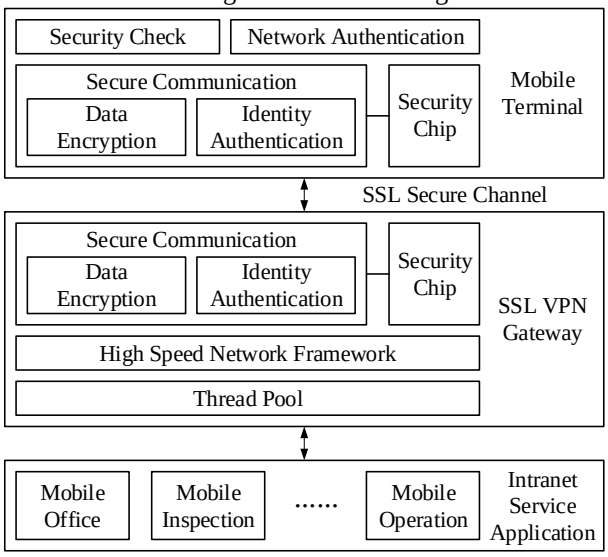

figure 8. mobile Terminal Security Protection Schematic

1) Safety Inspection Module

If a mobile terminal wants to access internal resources of an enterprise, it needs to carry out a security check in advance. Only mobile terminals that pass the security check are qualified to access internal resources, whereas mobile terminals that fail the check are prohibited from accessing internal resources of the enterprise.The security check module mainly reviews the operating system version of the mobile terminal and the disk files in special locations, and comprehensively judges whether the mobile device is qualified to access intranet resources according to the review results, so as to ensure the access security of the mobile terminal and eliminate threats from the source.

2) Network Access Authentication Module

Digital certificates issued by authoritative institutions are stored in hardware authentication cards, which have the functions of secure encryption and identity authentication. Enterprises will equip each person who goes out to work or has access to intranet resources for remote operation with corresponding hardware authentication cards, and will verify and identify their identity every time they connect to intranet for network access, so as to prevent the accessed mobile terminal from being a forged illegal user.

3) Safety Communication Module

The function of the secure communication module is to establish a secure channel using the State Security SSL communication protocol and the secure gateway. Its purpose is to ensure the security of the transmitted data. The module mainly uses cryptographic algorithms such as State Security SM1, SM2, SM3, SM4 to protect the transmitted data and ensure the authenticity, confidentiality and integrity of the data [17-19].

V. CONCLUSION

This article first analyzes the characteristics of mobile terminals in power companies, and elaborates on the current research status of SSL VPN technology based on the power industry. Secondly, according to the characteristics and requirements of information security construction in the power industry, an electrical security gateway based on SSL VPN technology is designed and implemented. The gateway is designed in accordance with national secret standards. Certified. Finally, a specific design scheme for mobile terminal secure access is given to ensure the security and credibility of mobile terminal access. It has certain practical significance for the information transmission and internal resource security protection of power companies.

REFERENCES

[1] Wu Kehe, Cui Wenchao, He Jianping. Mobile Security Access Platform for Power Enterprises[J].Computer Sys-tems,2014,23(07):31-36.
[2] Duan Zhuoran. Design and Implementation of User Rights Management Module for SSL VPN System [D]. Beijing University of Posts and Telecommunications, 2008.
[3] Yang Yang, Hua Liang, Zhou Lu. Design and Implementation of Secure Access Platform Based on SSL VPN [J]. Information Security and Technology, 2013,4(09):34-36.
[4] Xia Yuanzhen, Wang Lei, Wang Lingmin. Application and Implementation of VPN System in Power Industry APP[J]. Information & Communica-tions,2016(03):113-114.
[5] He Bo. Design of Information Security for Distribution Network Field Operation System Based on Mobile Inter-net [D]. North China Electric Power University (Beijing), 2016.
[6] Zhao Zhanling, Hu Wei, Han Yu. Research on Design and Implementation of VPN Security Gateway [J]. Information System Engineering, 2019(01):71.
[7] Hou Yan. Research on Computer Network Security De-sign Based on SSL Protocol[J].Computer Programming Skills & Maintenance,2019(05):147-148+167.
[8] Shi Lu. Application and Development of VPN Technology [J]. Information Security and Communication Secrecy, 2010(2):56-58.
[9] Xu Guangyu. Resource Sharing and Security Regulations of Distant Local Area Networks [J]. Information Network Security, 2010 (09): 57-58.
[10] Suo huawei. Deployment and Practice of VPN Network Construction in Hydropower Construction Enterprises [J]. Water Conservancy and Hydropower Construction, 2013 (03): 109-112.
[11] Zang Hongguo. Application analysis of the design scheme of SSL VPN system for operator business terminal[J].Science and Technology Economic Guide,2015,23(2).
[12] Cheng Rui. Research and implementation of terminal security access management system based on libevent architecture [D]. North China Electric Power University (Beijing), 2017.
[13] Min Yunlang. Design and Implementation of Secure Communication Protocol for Distribution Service [D]. North China Electric Power University (Beijing), 2018.

[14] Xia Bin, Du Shouguo. Network Design and Practice of Cloud Service Platform Load Balancer[J].Computer Ap-plications and Software,2014,31(08):121-125.
[15] Yan Jia, Li Chun, Xu Zhaoqing, Wang Dong, Wang Jia. Research and Application of Mobile Terminal Security Access in Power Grid Enterprises[J].Jilin Electric Pow-er,2014,42(06):17-19.
[16] Pang Wei. Comprehensive design research of public security mobile police system [D]. Tianjin University, 2012.
[17] Zhang Yun. Research and implementation of power marketing terminal security access system [D]. North China Electric Power University, 2013.
[18] Mu Hongtao. Research and Implementation of Distribution Network Security Interactive Gateway Based on State Security Algorithm [D]. North China Electric Power University (Beijing), 2017.
[19] Zheng Liancheng. Design and implementation of centralized supervision system for agent-based mobile terminals [D]. North China Electric Power University (Beijing), 2016.
[20] Wang Zhiyong. Application of SSL VPN Security Key Technologies [J]. Wireless Internet Technology, 2019,16(09):21-22.