Journal of Electronic Research and Application

Research Article

How to Achieve Both "Physical Isolation" and "Secure File Transfer" under the State of Strong Supervision

Min Ai*, Donglin Zhu, Yingli Zhang, Wan Tao, Xin Wei

Industrial Bank Co., Ltd. Harbin Branch, Harbin 150001, Heilongjiang Province, China

Abstract: Communication security involves all aspects of the country and society, and financial security is of top priority. Through strong supervision and strong technical means, a "semaphore" file exchange station is established. The data transmission system is composed of a sending server, a receiving server, and a "semaphore" communication box. Physical connections between internal and external networks are eliminated to achieve the purpose of "physical isolation" and "secure file transfer".

Key words: "Semaphore" file exchange station; Physical isolation; QR code transmission

Publication date: September, 2020

Publication online: 30 September, 2020

Corresponding author: Min Ai, 18646276959@163.com

1 Project Background

According to the "Administration of the Maintenance of Secrets in the International Networking of Computer Information Systems Provisions " promulgated and implemented by the Chinese State Security Administration on January 1, 2000, the Article 6 states that: " Computer information systems involving State secrets may not be directly or indirectly connected to the Internet or other public information networks. They must be physically isolated." The so-called "physical isolation" means that there can be no direct physical connection between the "intranet" and the "external network" of the relevant unit at any time. The network can be truly protected to prevent hackers from intruding and causing data loss.

Under the strong supervision of the state, the financial industry has issued a series of related regulations, which stipulate that the internal network of each commercial bank should be physically separated from other networks (hereinafter referred to as: network A and network B). However, in the case of complete physical isolation, the network A and the network B cannot perform inter-transfers of files, and it is difficult to carry out the business that requires file transfers. The original method of data exchange uses the following solutions:

1.1 Complete physical isolation

Use manually removable media to burn or copy the data or files of Network A to the removable storage media, and then manually load the data to Network B after safe processing. Although this method realizes the physical isolation between the network A and network B, it has the disadvantages of high resource consumption, low efficiency, difficult management, ease of copying data in multiple places or even out of the supervision area, and the spread of viruses and Trojan wares.

1.2 Use logic-gated isolation

That is, network A and B are connected by one-way import equipment, such as an air gap or a FGAP. Although it is efficient, it is not complete physical isolation and does not meet the current national requirements for the safe exchange of internal and external network data.

In response to the above situations, combining the QR code transmission technology with the industry application development platform, the project team created a "system for data transmission using QR code image recognition technology" (hereinafter referred to as "semaphore" file exchange station) based on intelligence, controllability and security to serve as an effective supplementary solution.

2 Project Functions and Novelties

The "Semaphore" file exchange station meets the requirements of industry's network management regulations. The product accessories are all industrial-grade designs, and the failure-free cycle of the main accessories can reach 20,000 hours. Specific functions and innovations are as follows:

(1) The transmission direction of data is customized as one-way transmission.
Network A is the user file upload terminal, and Network B is the user file download terminal. Reverse or two-way file transmission is prohibited. There is a complete physical isolation mechanism between Network A and B, and there is no direct communication channel between the two networks, ensuring data security.
Continuous display of QR codes between different security domains and the use of QR code reader to read the QR code data on the display as the transmission medium to achieve safe and controlled information exchange.

(2) The display and reader adopt a completely non-contact mode to for data display and reading.

(3) The system can log the user's file upload and download actions and can keep track of every step and trace the source of all users' operations.

(4) The system only allows uploading of files encrypted by document security software.

3 Outline Design of Project Application Platform

The web terminal of "Semaphore" file exchange station is developed based on the basic JEE application platform. The application development platform is the industry's mainstream project application research and development platform. Its advantage lies in the rapid response of the development of safe and stable JEE application systems, greatly shortening the development time of complex application systems and increasing the level of software reuse. Good technical support can be provided from the early project architecture design and research and development to the later project operation, maintenance and management.

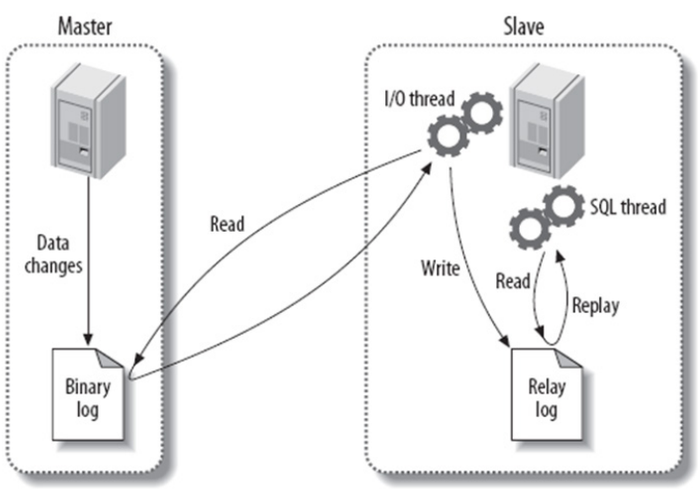
The underlying database of the sending server and the receiving server adopts a master/slave model, that is, real-time business data writing and updating operations in the master database, and the slave database will immediately synchronize the corresponding information. The specific process of the master/slave model is as follow：

(1) Any modifications in the master server will be inserted into the Binary log in real-time through the I/O tread of the master server.

(2) The Binary log of the master server is scanned from the server in real-time. If new data is found inserted into the Binary log, the resulting new Binary log will be written into the local Realy log.

(3) The slave server scans the Realy log regularly through SQL thread. If there is a new Binary log, it will immediately execute the same operation of the master server on the database.

In this way, the underlying data information of the master/slave servers is completely synchronized. The specific process is shown in the figure:

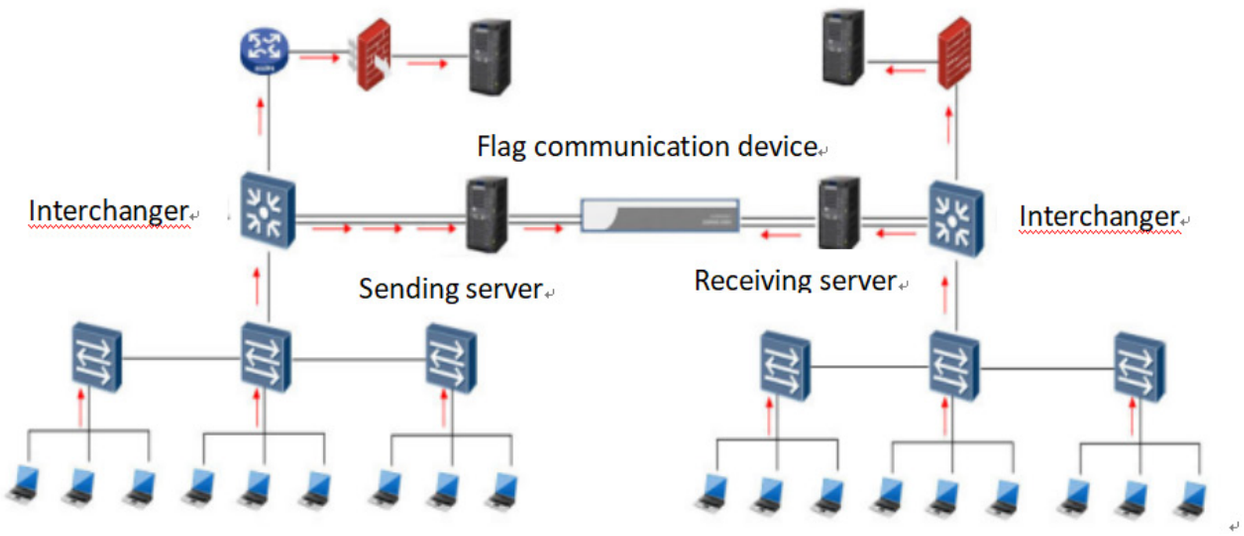


The user logs in to the "Semaphore" file exchange system on network A and upload the required DSM encrypted files. Upload information includes: uploader's name, file name, sub-branch/department, upload date.

After receiving the upload instruction, the “Semaphore” communication box transmits the file via QR code. Users can then download the file on B network B.

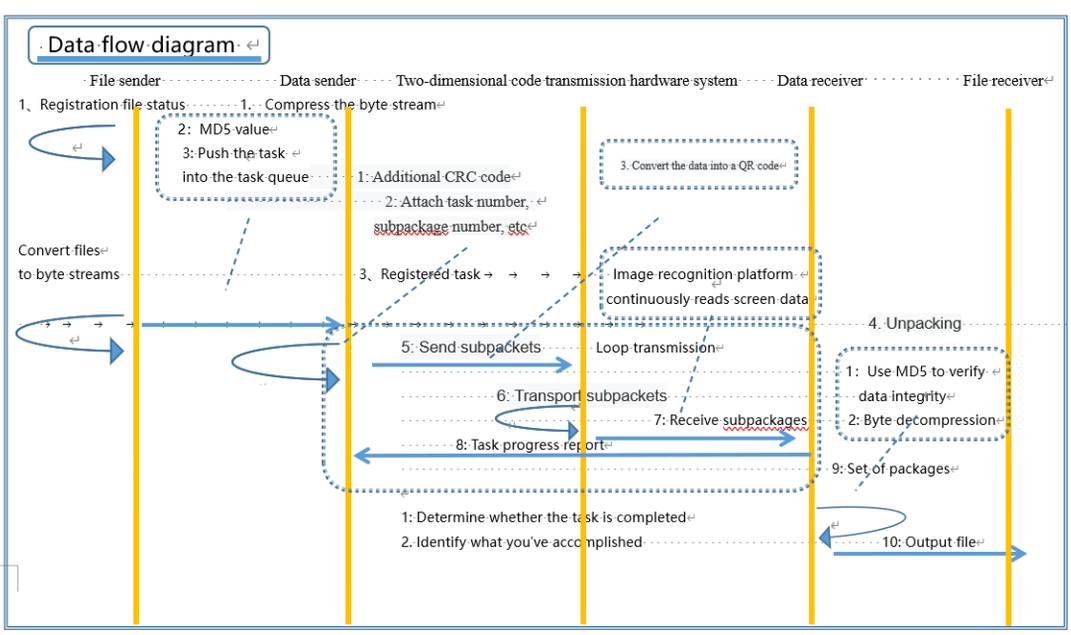
4 Project Architecture Design

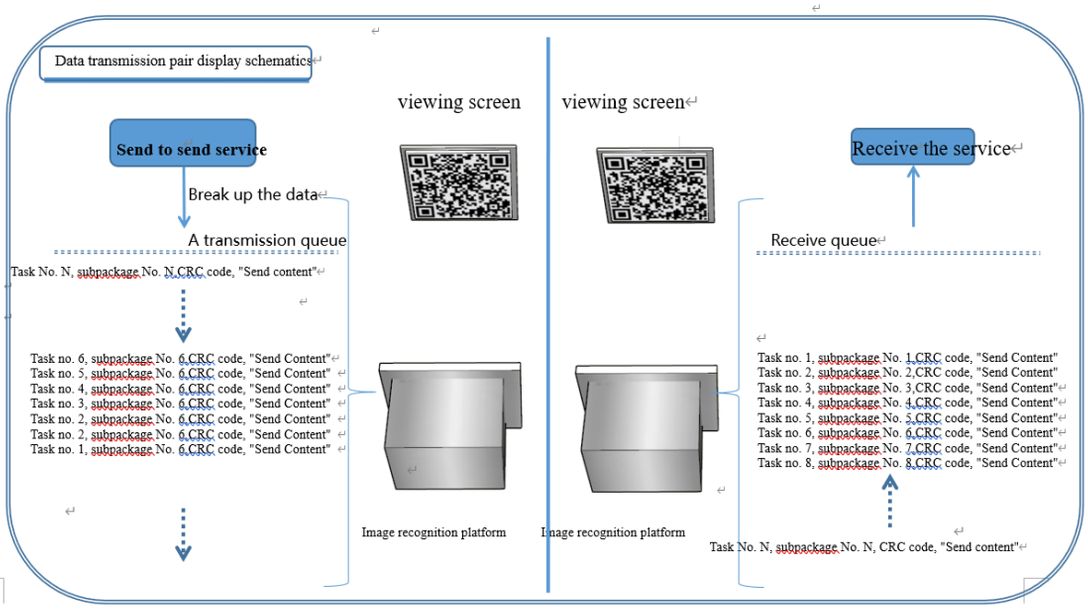
“Semaphore” file exchange station adopts B/S architecture design, and the overall system deployment architecture is shown in the figure below：



The system automatically converts the file uploaded by the user into a byte stream, and the bytes are compressed during the byte stream conversion. The MD5 value of the uploaded file is calculated, and a sending task is established and pushed in the sending task queue. The system unpacks the byte stream according to the size of the file to be sent, and at the same time unpacks each small packet that has been split up, and adds CRC code, task number, and subpacket number, etc. The number of unpacking varies with the size of the data. The transfer server converts the byte stream data of the sub-package into a QR code and displays it on the sending screen in parallel. The receiving end uses a QR code scanner to scan the QR code on the sending end screen by parallel communication for data reception. Each group of sub-packages received undergoes a verification process. After all sub-packages are received, they are packaged in a uniform manner, and MD5 is used to verify data integrity when grouping the packages. After the data are verified to be consistent, the complete file is exported to the designated location of the receiving end.

The schematic diagram of the data transmission process and the queue diagram are as follow:





The data transmission system is mainly composed of three parts: sending server, receiving server, and the "semaphore" communication box.

4.1 The hardware of the "semaphore" communication box is mainly composed of three parts (motherboard, display, and scanning reader)

（1） Motherboard Part： The motherboard is the core of this product. In order to ensure network security, data confidentiality, and product irreplaceability, the design and core software of the motherboard are all independently developed and customized by the Science and Technology Department of our bank. The main chip adopts industrial-grade ARM Cortex-M4 high-performance microcontroller core. This microcontroller uses a 90-nanometer manufacturing process and a self-adaptive real-time memory accelerator. The use of self-adaptive real-time memory accelerator technology is to allow the immediate execution of the kernel program, so that efficiency can be increased when the program is executed, and the performance of the microcontroller can be maximized. The self-adaptive real-time accelerator can unleash the full potential of the microcontroller core; when the CPU is operating at a frequency of less than 168MHz, the program running in the flash memory can achieve a performance equivalent to zero waiting cycle. The microcontroller integrates single-cycle DSP instructions and floating point unit (FPU) to improve the computing power and perform some relatively complex calculations and control tasks. The microcontroller utilizes multiple AHB bus matrix and multi-channel DMA technologies to support program execution and parallel processing of high-volume data transmission, increasing the data transmission rate. In order to ensure low power consumption of the device, the main chip supply voltage is set at 3.3V, and the external interrupt supply voltage is 5V (when the serial port chip does not trigger the interrupt, the interrupt pin is pulled up to 5V). The motherboard network chip is W5500, built-in with WIZnet full hardware TCP/IP protocol stack. The adoption of hardware protocol stack is to prevent the device from being attacked on the network and render data transmission safe and stable. The motherboard network connection uses an independent hardware Socket protocol to ensure that data communication does not affect each other. The TCP/IP packet processing is completed by a 32KB cache chip, and it integrates 802.3 Ethernet MAC and 10M/ 100M Ethernet PHY. This network chip has low power consumption, the maximum working temperature is around 40℃, and it supports power-down mode and UDP network remote wake-up. The working voltage of this chip is 3.3V, the I/O voltage is 5V, and the network supports auto-negotiation (10M/100M, full/half duplex). The two chips mentioned above use AMS1117 series voltage regulators for voltage stabilization. The serial port chip uses 5V power supply (maximum 5.3V). The main chip and the network chip are connected by SPI. The polling method is used to receive data. The number of motherboard-to-serial buffers is 4, each with 3000 bytes. The number of serial-to-network buffers is 4, each with 3000 bytes, and the number of receiving network buffers is 4, each with 2048 bytes. The maximum speed

from the main chip to the serial bus is 10M/s, and it can be expanded to 8USART at maximum. The hardware protocol stack is used to protect the device from attacks on the network and to make data transmission safe and stable. The server and the motherboard network connection uses an independent hardware Socket protocol to ensure that the data communication does not affect each other. The TCP/IP packet processing is completed by the 32KB cache chip, and integrated with the 802.3 Ethernet MAC and the 10M/ 100M Ethernet PHY. The network chip used has low power consumption and the maximum working temperature is around 40℃, and it supports power-down mode and remote wake-up from UDP network. The working voltage of this chip is 3.3V, the I/O voltage is 5V, and the network supports auto-negotiation (10M/100M, full/half duplex). The current baud rate is 115200. The working mode of the scanning-reader-to-host is the serial port chip enables FIFO (128 bytes) first-in first-out memory and enables FIFO64 bytes to trigger interrupts. The main chip stops reading from other processes when the interrupt is triggered. The received data is put into the buffer and sent to the host. The working mode of the host-to-screen is that the main chip polls the network chip port, puts the received data into the receiving buffer when it is available, then slices the data and adds the message, and sends it to the LCD screen.

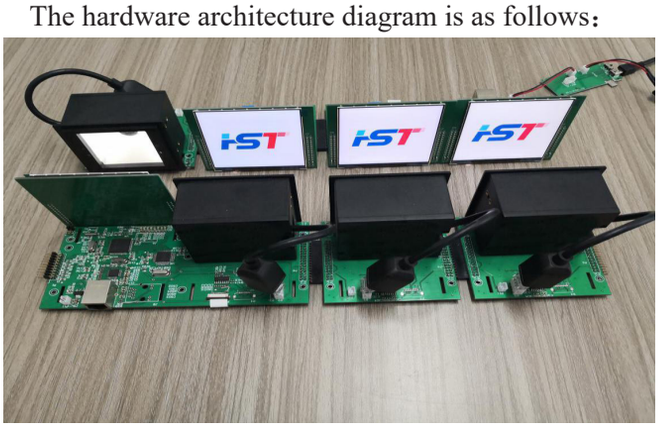
（2） Display Part：The display adopts industrial-grade screen, processor: 32-bit high-speed customized processor, data communication method is through serial port, baud rate is 115200, resolution is 720dpi*720dpi, screen brightness is 280cd/ ㎡ , power supply: 5V/250MA.

（3） QR Code Scanner：The scanner adopts an industrial-grade QR code reader and the sixth-generation core decoding technology. It can quickly read all kinds of large data-volume screen barcodes. The IP65 high protection level prevents foreign objects from intruding and can work continuously for 24 hours a day. Communication method is through serial port, baud rate is 115200 bps, image sensor is CMOS, resolution 800dpi*800dpi, working voltage 5V, reading accuracy ≥ 3mil.

4.2 The Implementing Methods as follow：The sending server sends the data to the “semaphore” file conversion system, and the received data is converted into bytes. The motherboard system sends the bytes to the display through the serial port, and the display converts the data into a QR code for display.

The scanner at the receiving end reads the QR code on the screen to form byte data, which is sent to the motherboard system through the serial port. The motherboard system transmits the data bytes to the receiving end server through the network. The receiving server system verifies, decompresses and organizes the received data to yield the document.

The hardware architecture diagram is as follows：



5 Conclusion

This paper briefly introduces the “semaphore” file exchange station. The use of QR code for data transmission between isolated networks ensures the reliability of the data while taking into account the security of the data.

References

[1] Standards Press of China. Barcode national standard compilation [s]. Standards Press of China，2004.

[2] Yi W. Introduction to the application and standardization of QR code barcode technology [J]. China Standardization，2006.

[3] Rav-Acha, AY. Pritch P, Peleg S. Making a Long Video Short: Dynamic Video Synopsis[J]. Proc. IEEE Conf. Computer Vision and Pattern Recongnition, June 2006.

[4] Yu Y. Bar code and automatic identification technology[J]. Enterprise standardization, 2002.