

Research on a Cotton Storage Platform and Security Strategy Based on IoT

Zhao Xiaodong, Li Yajing

*Institute of Information Science and Engineering, Hebei University of Science and Technology,
Shijiazhuang, China.05001
Email: zhaoxiaodong@hebust.edu.cn*

Abstract: *Establishing cotton storage IoT can realize real-time, unified management of the national cotton storage, which has an important strategic significance. This paper describes the application system of cotton storage IoT and proposes an application platform architecture mixed with C/S and B/S. IoT development is still in its infancy, lacking a unified IoT system standard. Its system has some flaws, especially in its system security. This paper analyzes the security problems of the IoT system and offers some strategies for its research.*

Keywords: *Cotton storage, IoT, system platform, architecture, security strategy.*

1. Introduction

This study is based on the contents of “Twelfth Five-Year” National Science and Technology Support Project “Agricultural intelligent information systems and services platform based on IoT technology”. Cotton is the second largest crop and an important strategic material in our country. Guaranteeing the quality, the hoarding amount and the amount of import library of the national cotton warehousing in real-time and the accuracy is directly related to the cotton pricing for the overall market and price forecasts. It can provide data supporting for the import and export, warehousing logistics optimization allocation and national policies. Establishing the application platform of cotton storage IoT can realize real-time, unified management of the national cotton storage, which has an important strategic significance.

The application of a cotton storage system platform enables more uniform and efficient management, and by using C/S and B/S mixed-mode to build an

application platform can improve the security, reliability and stability of the system. But with the extensive application of IoT, it may also bring security problems. For example, some smart devices lack security in the perception layer; the connecting to the network is not protected at the transport layer; the controlling and operating have no security protection measures at the application layer. It is easy to provide a way to attack or tamper by the information about malicious attackers, thus affecting the normal operation of the system. Therefore, it is particularly important to ensure efficient safety protection measures. This paper designs an application platform for cotton warehouse IoT. At the same time it makes a strategy research on the security problems at the perception layer, the transportation layer and application layer of IoT.

2. Application system and architecture designing

2.1. Application system

The overall structure of the cotton storage IoT system diagram is shown in Fig. 1.

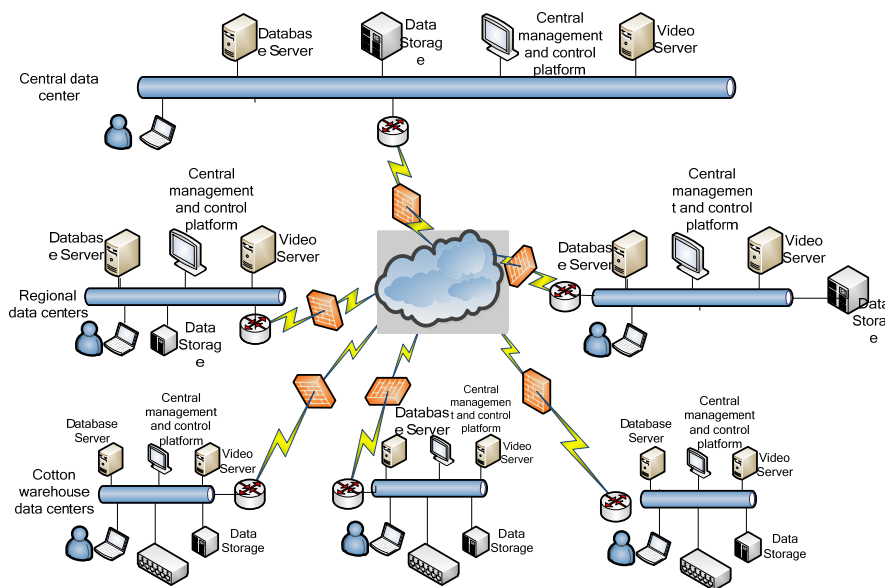


Fig. 1. The system overall architecture diagram

In this system, the cotton storage features monitoring information, as well as the hoarding amount and the out of the library data store in the database servers and the video streaming are exclusively stored in the video server. A single server pattern often leads to system paralysis, and it cannot already meet the needs of a large system. Building a virtual platform in the background server of the system, packaging the operating systems, application programs and the server in virtual machine files, allowing more virtual machines running on a single hardware server, which allows the server to even a few hundreds of virtual servers, isolated from each other, can improve the maintainability and scalability of the system. It can also

satisfy the user in supporting health diagnostics, configuration backup and restore, rollback and recovery protocols and provide more network functionality and more powerful cloud-based features by using cloud computing technology to solve the problem of the mass data storage, retrieval without being abused.

The deployment of the application system points at two levels of a cotton warehouse in a local and central data center. All across the country, the local cotton storehouse stores information of the video server and the database server transfers to the central data center in real-time, and uses the synchronization mechanism to make the local synchronize with the central data center, and to realize the two levels of real-time monitoring and history going back. The application platform points the warehouse management and monitoring information system of cotton warehouse characteristics. Warehouse management is doing real-time statistics for the hoarding amount and the out of the library, the management department can keep track of any cotton warehouse storage conditions, and provide decision support for the import and export of cotton, the optimization of logistics distribution and the national policy. The monitoring system of cotton warehouse characteristics is doing a real-time monitoring for the cotton warehouse environment, such as temperature, humidity, illumination, video information, quality analysis and so on. It calls the alarm message for abnormal condition, and provides information about ventilation, fumigation and drying. It not only guarantees the quality of the cotton, but also achieves analysis and summary for the storage environment in different areas of the country.

2.2. System architecture design

The architecture of the commonly used application software has two types, namely the C/S (Client/Server) architecture and B/S(Browser/Server) architecture.

C/S can make full use of both ends of the hardware environment and distribute tasks reasonably to the Client side and the Server side. C/S is generally set up on a Windows platform and dedicated network, and applied to the small scale of the network environment. Its biggest advantage is geared to the fixed user group, and can also make a multi-level check for permissions, and has a very strong controlling ability for information security. But if C/S can be run, the customers must install the C/S client, which is typically a centralized mechanical processing and the interactivity is relatively low. Due to the integrity of C/S application, the system upgrade is more complex. The system updates are likely to do a whole new system.

B/S user working interface is implemented via WWW browser and B/S achieves logging in web and remote monitoring by ASP.NET + SQL database technologies. Its biggest advantage is based on a wide area of networks, suitable for a large system platform. At any time, in any place and in any system, as long as you can surf the Internet, you can communicate with users with rich vivid expression, which has a stronger adaptation range than C/S. The system maintenance and the upgrading is simple, as long as the user download installation can be achieved. Nevertheless, B/S faces a unknown user group and has a relatively weak control ability for information security.

Integrating the advantages and disadvantages of B/S and C/S by using the hybrid architecture pattern of combining C/S and B/S structure we can have a combination of two different structure characteristics [2]. Not only can it solve the different regions and different networks users access to the system conveniently and robustly, but also is conducive to robust software architecture, upgrading software usability, improving the work efficiency [4]. Therefore, in this study the application platform of the cotton storage IoT uses the architecture pattern of combining C/S and B/S structure. For data browsing all adopt B/S structure, the safety of system controlling uses C/S, and the part of involving the data modification is implemented in C/S. This will not only prevent hackers trying to attack the system, but also ensures that the data transmission is smooth in real time and improves the reliability and stability of the whole system greatly.

The system of C/S model is used for modifying and setting global information by the central personnel. The design of the system is divided into a regional management module, a role management module, a management module, an authority management module and user management module. The system can access and control the information of all cotton library, including the generating role, produce cotton library administrators, alarm management, equipment management and so on. Local application is responsible for local user management, planning role, device management and cotton warehouse management. The system of B/S model is mainly used for browsing the data with permissions by legitimate users. In B/S system, the central personnel according to assigned permissions to access the whole cotton library information, and the local cotton library staff only has access to the local system. The display of the central system includes real-time data, history inquiry, event handling, quality analysis, log management, system management and a system help module. The display local system includes real-time data, history inquiry, incident reporting, quality analysis, log management and system help, etc., B/S and C/S modes of combination of the architecture diagram is shown in Fig. 2.

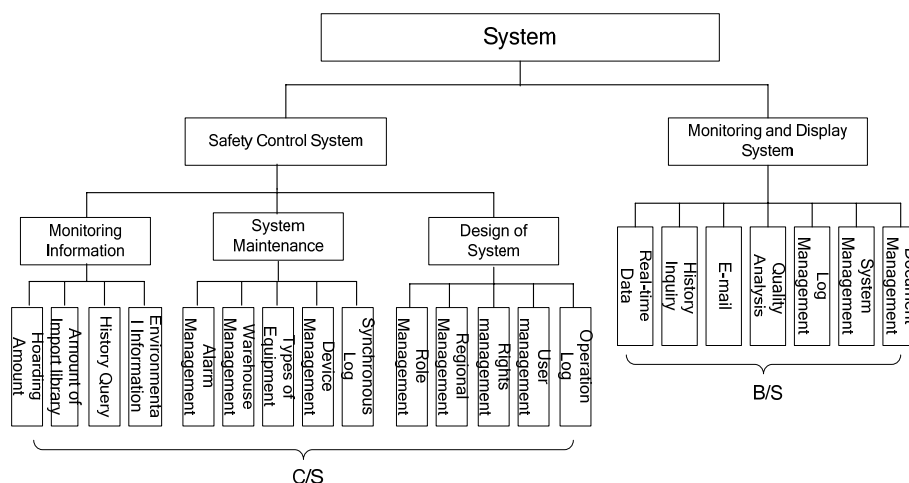


Fig. 2. B/S and C/S mode of the architecture diagram combination

3. Research on security policy of cotton storage IoT system

IoT system security includes physical security, network security, information content security and infrastructure, security, etc. The main objective is to ensure the integrity and confidentiality of information, to ensure the users' control of the system and to ensure the operation of the system safely, stably and reliably. From the perspective of information processing of the IoT, the information fusion after collecting, gathering, transmission, decision-making and control process, can be divided into three levels: perception layer, transportation layer and application layer. From the perception layer up to the application layer, every level has security flaws, the system information security issues facing the situation are very strict in the field of IoT. In this system, in order to ensure the cotton storage network system security and reliability, at the perception layer, the information collection devices which on the front-end are coded and uniquely identified, using the identity mechanism to identify each device, as to ensure that data is not tampered during the acquisition process. At the transport layer, the information is encrypted, and through a virtual professional network channel it achieves network interconnection between the local cotton storehouse and the central data center. At the application layer, the terminal installs a secure desktop software, and the log user implements hierarchical privileges to access, to improve the safety of data terminal equipment.

3.1. Security policy of the perception layer

At present the equipment function of the perception layer is relatively simple and has no complex ability of security protection. While the sensing device is varied, including temperature and humidity sensors, light sensors, video collection equipment (a camera). Even there is variety of data collection to monitor the whole process of the equipment, they have no specific standard. It also cannot provide a unified security mechanism. In this study, through secondary development for the equipment, which is the equipment coding identification for every equipment, and equipment and coding is one-to-one correspondence to achieve the only equipment coding standard in the whole system. As a symbol of system accessing, using the identity mechanism to ensure the data of every equipment can be identified and recognized, to prevent the use of a terminal network intrusion.

In the system the acquisition equipment encoding rules according to the cotton library district code in provinces and cities, the cotton base sequence number, the cotton warehouse sequence number, the equipment type and serial number to set, constituting the only code of the acquisition device. Among them, the cotton library district code in provinces and cities is shown with the local postal code (5 bits), to assure that each cotton library region encoding keeps in touch with the region postal code within the system. The cotton base sequence number is shown in Table 1. The cotton warehouse sequence number is shown in Table 2. The device type code is shown in Table 3. The equipment serial number is shown in Table 4.

Table 1. Cotton library sequence number

Cotton library name of XX region	Coding
C1 Cotton library	01
C2 Cotton library	02
...	...
Reserved	10-FF

Table 2. Cotton warehouse sequence number

Cotton warehouse name of XX region	Coding
No 1 Cotton warehouse	01
No 2 Cotton warehouse	02
...	...
Reserved	10-FF

Table 3. Device type code

Device Type	Coding
temperature sensor	W
Humidity sensor	S
Light sensor	G
video monitor	L

Table 4. Device sequence code

Device sequence	Coding
No 1 Device	01
No 2 Device	02
...	...
Reserved	FF

By encoding the rules, this guarantees that each collection equipment number is unique in the whole system, such as No 2 temperature sensor device in No 5 cotton storehouse of Hebei Nangong C2 cotton library. The postal code of Hebei Nangong is 51800, C2 cotton library coding is 02, No 5 cotton storehouse coding is 05, the temperature sensor coding is W, so this equipment coding is 51800 02 05 W 02. The No is the only equipment coding in the cotton storage IoT system.

3.2. Security policy of the transport layer

Since the management system includes two levels of management: cotton storehouse and central data center, it is necessary to implement the data through the network transmission in order to realize the central data center to remote controlling all cotton storehouses from all over the country. Public web has a fast connection speed, short transmission delay and high accuracy. But because of the strong transparency of the network, just using the public not taking measures to protect the information, it is easy to be stolen and attacked in the transporting process, and it is

also more likely to be interfered, and will directly affect the security of the system. Therefore, using the data encryption technology and VPN technology to realize the transfer security from a local cotton data storehouse to the central data center at the transport layer of this system ensures that the data is not being attacked or tampered by a third party during the process of transmission.

3.2.1. Data encryption technology

(1) Symmetric encryption algorithm

Symmetric encryption algorithm is also known as a traditional cryptographic algorithm, most of the encryption key and the decryption key used by symmetric encryption algorithm are employing the same algorithm, that is, according to the encryption key, the decryption key can be calculated and vice versa. Before the two sides communicate, you need to set up a key. The confidentiality of the key determines the security of the arithmetic. Once the key is compromised, the third party will get the key to decrypt information, thus, causing leakage of information or being tampered. Thus a security risk exists in the symmetric encryption algorithm.

Data Encryption Standard (DES) [13] was published by the US National Institute and Technology (NIST) in the mid-1970-ies, and its source was the cryptographic algorithm from IBM, with one symmetric key block encryption password. DES is a symmetric key block encryption password, with great efficiency of encryption and high speed, which is suitable for large volume data transmission.

DES processes 64-bit plain text M while generating 64 bits cipher text C . The efficient length of key K is 56 bits; rather, the actual length of the key K input is 64 bits, among which 8-bit (8, 16, ..., 64) is used as parity bit. Before performing the round encryption, firstly, an Initial bit Permutation (IP) should be performed. DES encryption algorithm conducts a total of 16 rounds of encryption and each round has a 48-bit key K_i , totaling 16 sub-keys K_1-K_{16} ; in each round, 8 fixed alternative mapping boxes S_i (S boxes) from 6 bits up to 4 bits are used. For 64-bit plain text, it will be divided into two separate 32-bit plain texts, denoted as L_0 and R_0 . Then round encryptions will be performed. The algorithms in each round are the same, that is, 32 bits L_{i-1} and R_{i-1} in the previous round is used and 32-bit L_0 and R_0 is produced. Its specific encryption formula is

$$\begin{cases} L_i = R_{i-1}, \\ R_i = L_{i-1} \oplus f(R_{i-1}, K_i), \\ f(R_i, K_i) = P(S(E(R_{i-1}) \oplus K_i)), \end{cases}$$

where $1 \leq i \leq 16$; E is a fixed extension permutation, to achieve that 32-bit R_{i-1} is mapped onto 48-bit (all bits are used once, some are used twice); P is another 32-bit fixed permutation. Finally, the inverse Initial Permutation IP^{-1} is re-arranged to produce a 64-bit cipher text.

DES encryption and decryption use the same algorithm, and the order of the decryption key is the opposite of the encryption key.

(2) Asymmetric encryption algorithms

RSA is a public key encryption algorithm [14], and a classic algorithm in non-symmetric encryption algorithm. The asymmetric encryption algorithms use different keys (a public key and a private key) when encrypting and decrypting, both of which are a pair with the encryption key public and the decryption key private. For example: if A must send a message to B , A uses B 's public key to encrypt the message. After B receives a message, it decrypts the message with its private key, and thus restoring the plain text. Since only B knows their own private key, the third party cannot decrypt the information. So it is more secure than the symmetric encryption algorithm.

RSA encryption algorithm is an algorithm based on integer factorization, whose process can simply be described as $n = pq$ ($p \neq q$). To calculate the pixel values p and q , the specific algorithm is:

1) randomly generate three integers p, q, r : p and q are two distinct primes; r and $(p-1)(q-1)$ are relatively prime; then p, q, r is the private key;

2) calculate the value of m to make $rm = 1 \pmod{(q-1)(p-1)}$; m and n are the public keys.

Set the plain text packet $m = (m_1, m_2, m_3, \dots, m_k)$, the corresponding cipher text is $c = (c_1, c_2, c_3, \dots, c_k)$, using the improved RSA algorithm [7] as follows:

Encryption algorithms: $c_j = m_j + m_{j-1} \pmod{n}, j = k, k-1, k-2, \dots, 2$,

$c_1 = m_1^e \pmod{n}$.

Decryption operations: $m_1 = c_1^d \pmod{n}$,

$m_j = c_j - m_{j-1} \pmod{n}, j = 2, 3, 4, \dots, k$.

Encryption and decryption are required to perform a first power operation and the $k-1$ additions remaining operations. As shown, RSA algorithm does well in a resisting decipher and it is safe.

(3) DES and RSA mixed encryption model

Table 5. The relationship between the confidentiality level and secret key

Level of confidentiality	DES key length (bit)	RSA key length (bit)	Secret life
80	80	1024	2010
112	112	2048	2030
128	128	3072	2040
192	192	7680	2080
256	256	15360	2120

Table 5 shows the relationship between the confidentiality level and secret keys of DES algorithm and the RSA algorithm [5]. DES and RSA at the same confidentiality level have different key lengths. RSA key length is ten times the length of the DES key, even dozens of times. Apparently, RSA is better than DES in privacy and security; with the improvement in the level of confidentiality, both RSA and DES key lengths are increasing, but RSA key length growth rate is greater

than that of DES. If a high level of confidentiality is required, RSA calculation will be very large and the calculation speed will be low.

By comparing the key lengths of RSA and DES algorithms, to ensure the security and speed of information encryption and decryption, combining the advantages and disadvantages of DES and RSA, a combination of both methods is used, i.e., DES key is encrypted with RSA based on DES encrypting plain text data. Set M be a plain text; C is encrypted as a cipher text; K_D is the key of DES encryption and decryption, K_{E2} is a public key of RSA, K_{E1} is a private key of RSA; DES's encryption process is denoted by f_1 , the decryption's process is denoted by f_1^{-1} ; RSA's encryption process is denoted by f_2 , the decryption's process is denoted by f_2^{-1} . The encryption model is shown in Fig. 3, the specific process being:

(1) the sending end generates the key K_D of DES algorithm, encrypts the plain text M to produce cipher text C_1 ;

(2) encrypts DES algorithm's cipher text using the receiving end RSA's public key K_{E2} to generate cipher text C_2 ;

(3) sends cipher text C_2 and the encryption key to the receiving terminal via the network;

(4) the receiving end decrypts the sent cipher text C_2 with the help of its own RSA decryption key K_{E1} and gets the original DES cipher text C_1 ; Since DES encryption and decryption keys are the same, cipher text C_1 is encrypted by DES key K_D to obtain the plain text M sent by the sender.

This can be expressed by the formula: $C_2 = f_2(f_1(M))$, $M = f_1^{-1}(f_2^{-1}(C_2))$.

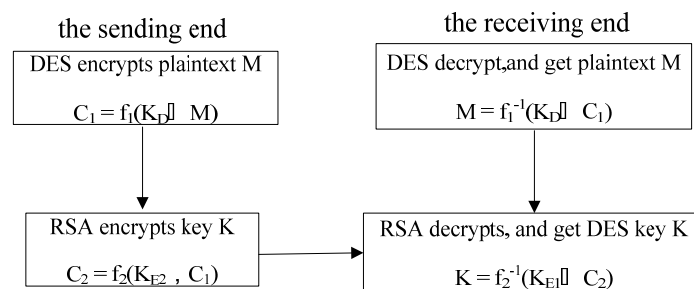


Fig. 3. Encryption model

DES and RSA have their own advantages and disadvantages. DES and RSA encryption algorithms are mixed in use not only to retain their advantages, but also make up for their shortcomings to reach relatively satisfactory results. Their advantages are as follows:

1) DES is suitable for data encryption of large amounts, DES encryption and decryption of information can maintain the efficiency;

2) RSA encrypting the keys generated by DES makes the security and convenience of storing the key guaranteed; even if a hacker steals any critical data, it is still difficult for him to obtain the required information, because all the data are encrypted and the data got by the hacker are garbled.

Because the algorithms that the system uses are a standard source, there may be a backdoor [5]. Additionally, the research in our country on cryptography is not

enough. Therefore, to ensure security of information at a deeper level, the network management should be intensified.

3.2.2. VPN technology

VPN technology is one of the main technologies to solve network security issues in recent years, with easy linking and low cost in operating, and connecting remote users, especially the data transmitted has high reliability. The high-level encryption and identification agreement can be used to protect the data against snoop, theft and other non-authorized users. Therefore, creating a temporary, secure, stable virtual private network channel in the public network to achieve internetworking between the local cotton warehouse and the central data center can make the data transmission fast and secure.

With the help of VPN equipment to design a monitoring system, a virtual local area network between the nodes and cotton internal Internet is established via VPN. During VPN access, using the private IP address that is assigned to the cotton local warehouse, monitoring all the hosts that spread over a wide area in the network can be achieved. IPSec VPN needs to install a specific device at the remote end-user side to establish a secure tunnel, so the border router in the local cotton warehouse can be used as IPSec VPN tunnel endpoints [16]. A VPN tunnel is established through the border security gateway between IPSec VPN and the central data center.

Security gateway is an organic fusion of various technologies, and it has an important and unique protective role, ranging from protocol-level filtering up to very complex application-level filtering. Security gateway itself has functions of firewall, antivirus, intrusion detection, user access active authentication and others. Secure gateway itself still has VPN functions and establishes a VPN tunnel to the database server; it also has a multi-network blocking function, that can only visit the protected network by a gateway after connecting the gateway client, that can block the other web page request to ensure the security of data transmission and access.

The security gateway is set up at the exit of the local network in the cotton warehouse, that is, the internal network port of the gateway connects to the local network in the cotton warehouse and the external network connects to the public network and the user is isolated from the protected network by a gateway. A security gateway deployment diagram is shown in Fig. 4. The user and client initiate a request to create a tunnel and then create it, at the transmitting end of the tunnel, the user enters a password to submit a digital certificate; an encrypted connection with the client (Central data center terminal) can only be performed after the gateway authentication, the data can be transmitted after being encrypted, the data transmitted are encrypted which have already been packaged; at the central data center side, the decision whether to allow the user (user or client) access or not, is made according to the access control, only the user (client) that has gained access to jurisdiction and passed the authentication can decrypt the transmitted data. In this way, the maximum security of information transmission is achieved with minimum investment without changing the structure of the network.

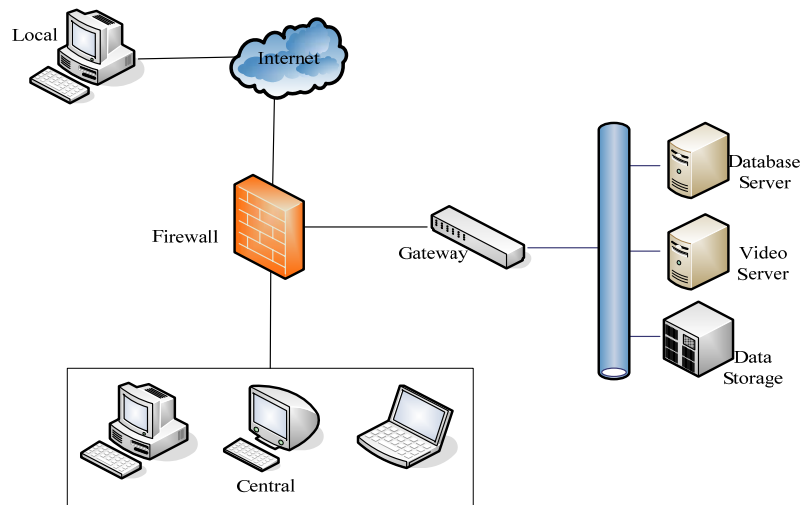


Fig. 4. A security gateway deployment diagram

3.3. Security policy of the application layer

Application layer security issues mainly come from the related business platform of various new businesses and applications. Large-scale, multiple platforms, many business types make the application layer security of IoT face new challenges. Malicious code and the software system vulnerability itself produce a great threat for the application system. At present, vast amounts of data information processing and business control strategy at the application layer have more bottlenecks in terms of security, for example, illegal intervention or internal attacks, loss of the equipment (especially the mobile devices). Aiming at information security, a hidden danger in the application layer, in a fixed computer terminal security desktop software is installed, and the log user implements hierarchical privileges to access, to improve the data security of terminal equipment at the application layer.

(1) Security desktop

Users (clients) install desktop security software on the computer. When users are using a client to access the security desktop software, they must insert USBKEY to login the system, and the need to pass strict user authentication, such as the accession number and the password must match, only passing the verification, the authorized users can access the information to prevent the illegal user's access. In the applications process of the security desktop, the user terminal without leaving any data, the data is stored in the background disk array, the users only need to consider protecting the background disk to prevent information leakage. So, using the algorithm of the data encryption storage, the probability of the front-end system platform causing information leakage will be greatly reduced.

(2) Hierarchical access

Statistically, at present the enterprise information leaks at least 60% from desktop security management within the enterprise. Therefore, facing all kinds of users, the enterprise internal desktop security management problem has become one of the biggest problems faced by information security.

The access permissions are associated with the role, and the role is associated with the users, so that it realizes the logical separation between users and the access permissions [3]. Therefore, introducing the role as inter-mediatory, the rights management can define the various roles according to the need, and set up the corresponding access permissions for the role. Due to the fact that the same jobs tend to be of the same or similar business, according to their job and responsibilities assigned to different roles, such as system administrators and ordinary users, so as to realize the logical separation between users and permissions, to ensure that resources are not being illegally accessed and used, to ensure the security of the system.

A user can be assigned to multiple roles, the role has the right to perform multiple functions, a function can be achieved by multiple web pages. After entering the system, different users see a different function menu. For the average user, the user management feature is not visible.

4. Conclusion

This paper, on one hand, introduces the convenient and efficient application system of cotton storage IoT, which uses the hybrid architecture pattern of combining C/S and B/S structure to design the application platform architecture. On the other hand, it also analyzes the security problems from the perception layer up to the application layer of IoT, and puts forward countermeasures to the security problem of every level, to prevent different kinds of hackers, viruses, Trojan and holes, respectively attacking on the perception layer, transporting layer and application layer. However, the security problem of IoT system is not a simple technical problem, it not only needs safety awareness by developers and users with higher requirements, but also requires a combination of strict and scientific management, decreasing the information security hidden danger to the whole Internet system to a minimum. IoT from the architecture to the development of security is still at its primary stage. Some system standards need to be further improved, for the challenge is facing more severe problems than imagined.

Acknowledgments: Project Support: Cotton storage environment monitoring information of remote acquisition, storage and display system (National Science and Technology Support Plan, 2012BAH20B030-4).

References

1. Yang, Jincui. Research on Key Technologies of Control Security in the Internet of Things. Beijing University of Posts and Telecommunications, 2013.

2. Liu, Jun, Yan Fang, Yang Xi. The Internet of Things Technology. Beijing, Mechanical Industry Press, 2013.
3. Long, Qin, Liu Peng, Pan Aimin. Research and Implementation of an Extended Administrative Role-Based Access Control Modle. – Research and Development of the Computer, Vol. **42**, 2005, No 5, 868-876.
4. Li, Wenjun. Research and Design of High School Educational Administration System Based on C/S and B/S Hybrid Architecture. Nanchang HangKong University, Nanchang, 2012.
5. Su, Kaiyuan. Research and Implementation of the Encryption Algorithm. Nanjing University of Posts and Telecommunications, 2012.
6. Li, Anzhi, Cui Wei, Xu Yonghong. A Authority Controlling Scheme in Web Accessing Based on Role. – Computer and Information Technology, Vol. **6**, 4-6, 46.
7. Xia Shuhua. Research on Data Security Transmission Technology Based on DES and RSA Encryption Algorithm. – Manufacturing Automation, Vol. **02**, 2011, 180-182.
8. Wang, Yan. Research on Key Technologies of Information Transmission for IoT Control System. Northeast Forestry University, 2012.
9. Zhang, Zejian. Internet Information Security Research. – Logistics Technology, Vol. **20**, 2011, 29-31.
10. Hong, Ren. Introduction to the Internet of Things Security Issues and Measures. – Computer CD Software and Application, Vol. **13**, 2012, 54-55.
11. Liu, Junbin, Wang Yong. Application of Multi-Campus Network Based on MPLS VPN. – Value Engineering, Vol. **3**, 2014, 188-190.
12. Sun, Lifei. Research on the Campus Network Based on VPN Technology. – Information and Communication, Vol. **1**, 2014, 103-104.
13. Hellman, M. E. DES Will Be Totally Insecure Within Ten Years. – IEEE Spectrum, Vol. **16**, July 1979, No 7, 32-39.
14. Rivest, R. L., A. Shamir, L. Adleman. A Method for Obtaining Digital Signatures and Public Key Cryptosystems. – Communications of the ACM, Vol. **21**, 1978, No 2, 120-126.
15. Atzori, L., A. Iera, G. Morabito. The Internet of Things: A Survey. – Computer Networks, Vol. **54**, 28 October 2010, Issue 15, 2787-2805.
16. Zhiyong, Luo, Bo You. Research on University Digital Library Formation Model Based on VPN Network. – Library Studies, Vol. **1**, 2013, 35, 52-59.