2015 The 5th International Workshop on Computer Science and Engineering
doi: 10.18178/wcse.2015.04.113

A Strategy Study about Security Strategy of Cotton Storage IoT System

Zhao Xiao-dong[1,a], Li Ya-jing[1,b], Li Hao[2,c]

[1]Institute of Information Science and Engineering, Hebei University of Science and Technology,
Shijiazhuang, 050018 ,China
[2]PetroChina Pipeline Compressor-set Maintenance, Repair and Overhaul Center,
Lang Fang, 065000, China

[a]zhaoxiaodong@hebust.edu.cn, [b]lyj9126@126.com, [c]li.hao28@yahoo.com

Keyword: Cotton storage, IoT, Security issues, Strategy.

Abstract. Cotton is the country's strategic material, and the information about cotton reserve is related to national strategy security. Any information leaks is most likely to cause damage on the security of national strategic reserve of cotton. Establishing cotton storage IoT can realize real-time, unified management of the national cotton storage, which has important strategic significance. But, IoT is a double-edged sword, it brings convenience to the control system, but also brings some security problems to be solved[1]. In order to ensure the safety of the information about cotton storage IoT system, for the security problems of cotton storage IoT system, this paper makes strategy research in three levels including the perception of the Internet layer, transport layer and application layer. The security of information is achieved without changing the structure of the network.

Introduction

This study is based on the contents of "Twelfth Five-Year" National Science and Technology Support Project " Agriculture 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 accuracy is directly related to the cotton pricing for the overall market and price forecasts, and it can provide a data supporting for the import and export, warehousing logistics optimization allocation and the national policies. Establishing application platform of cotton storage IoT can realize real-time, unified management of the national cotton storage, which has an important strategic significance.

Today, the development of the IoT is still in its infancy, the IoT system lack of unified standard, the system also has certain defects, especially the system security is more prominent. For example, some smart devices lack security in the perception layer; the connecting to the network are not protected in the transport layer; the controlling and operating have no security protection measures in the application layer. It is easy to provide a way to attack or tamper with the information for malicious attackers, thus affecting the normal operation of the system. Therefore, it is particularly important to make an effective safety protection measures. This paper makes a strategy study about security problems in the perception layer, the transportion layer and the application layer of cotton storage IoT system.

The cotton storage IoT system

The overall structure of the cotton storage IoT system diagram is shown in Figure 1.In this system, 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 exclusively stored in the video server. The deployment of the application system points two levels of cotton warehouse local and central data center. All across the country, local cotton storehouse stored information of video server and database server transfers to the central data center in real-time, and uses the synchronization mechanism to make the local synchronize with central data center, and to realize the two level real-time monitoring and history going back.

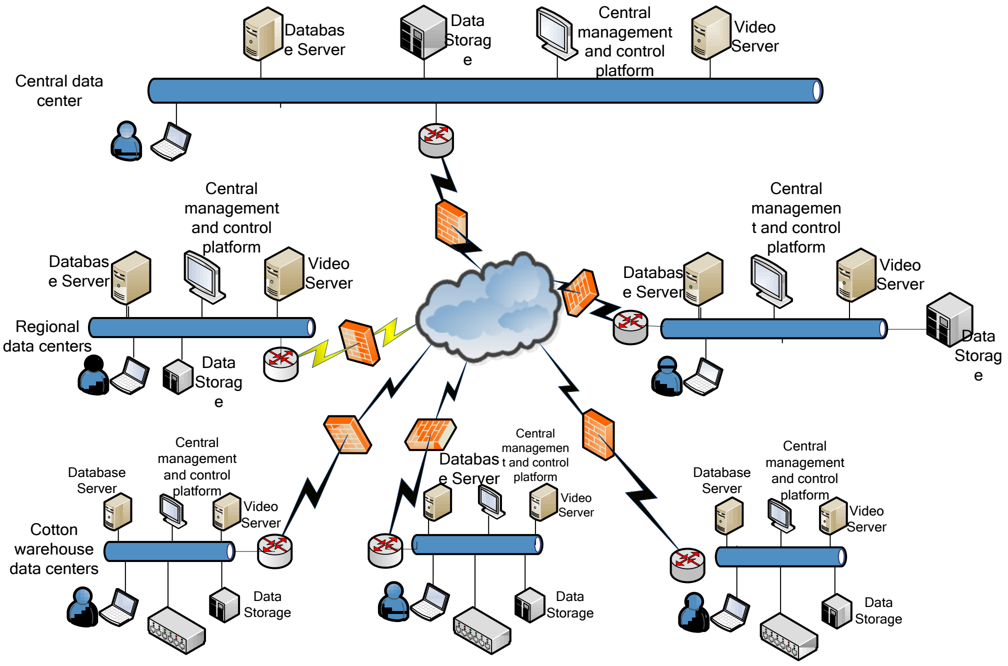

Fig.1 The System's Overall Architecture Diagram

Reaserch on security policy of cotton storage IoT system

The purpose of the study about IoT information security technology is to ensure the security of summary data transmission, storage, processing and access under the IoT environment[9]. 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 that users control on the system, and to ensure the operation of the system safety, stably and reliably. From the perspective of the information processing of the IoT, the information fusion after collecting, gathering, transmission, decision-making and control process, it can be divided into three levels: perception layer, transportation layer and application layer. From the perception layer to the application layer, every level has security flaws, the system information security issues facing the situation is very grim in the field of IoT.

In this system, in order to ensure the cotton storage network system security and reliability, in the perception layer, information collection devices which on the front-end are coded and uniquely identified, using the identity mechanism to identify each device, so as to ensure that data is not tampered during the acquisition process. In the transport layer, the information is encrypted, and through virtual professional network channel to achieve network interconnection between the local cotton storehouse and the central data center. In the application layer, terminal install secure desktop software, and the log user implement hierarchical privileges to access, to improve the safety of data terminal equipment.

Security policy of perception layer. At present the equipment function of 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 (camera). Even from a variety of data collection to monitor the whole process of the equipment, they have no specific standard. It also can't 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 recognition, to prevent the use of terminal network intrusion.

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

Table.1 Cotton Library Sequence Number

Ctton library name of XX region	Coding
C1 Cotton library	01
C2 Cotton library	02
……	……
Reserved	10—FF

Table.2 Cotton Warehouse Sequence Number

Ctton 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

As encoding the rules, that guarantees 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, 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.

Security policy of transport layer. In the transport layer of this system, using the data encryption technology and VPN (Virtual Private Network) technology to realize to transfer security from local cotton storehouse data to the central data center. The management system includes two levels management: cotton storehouse and central data center. Cotton warehouse where the local level throughout the country, its scope and the number of relatively is large, In order to China Cotton Group as an example, so far, in Xinjiang, Shandong, Hebei, Henan, Hubei, Anhui, Jiangsu and other the main area of cotton production and marketing, it has been under the jurisdiction of the cotton and 16 depot store and more than 160 libraries.

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, just to meet the needs of the system. But because of the strong transparency of the network, if just using the public not to take measures to protect the information, it is easy to be stolen and attacked in the transporting process, and it will directly affect the security of the system. Even relating to the import, export, distribution and national strategic information to optimize storage and logistics of cotton. In order to guarantee the security of information without affecting the transmission speed and accuracy of the information, the data is first encrypted and then establish a virtual private network access over public networks, to ensure that the data is not being attacked or tampered by a third party during the process of transmission.

1.Data encryption technology. Information monitoring system includes all the country's cotton warehouse storage data (including cotton, cotton storage time, and out of the library amount and hoarding amount) and environmental characteristics monitoring data (including temperature, humidity, light, video, quality analysis, etc.), it is a large amount of data. 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（Data Encryption Standard，DES）[7] is a traditional cryptographic algorithms, but most of the encryption key and the decryption key used by symmetric encryption algorithm are employing the same algorithm. Once the key is compromised, according to the encryption key the decryption key can be calculated and vice versa. So, a security risk exists in the symmetric encryption algorithm, causing leakage of information or being tampered. Asymmetric encryption algorithms use different keys (the public key and private key) when encrypting and decrypting, both of which are a pair with the encryption key public and the decryption key private. RSA is a public key encryption algorithm[8], and a classic algorithm in non-symmetric encryption algorithm. If you want to send a message, the sender uses public key to encrypt the message. After the receiver receives the message, he decrypts the message with his private key, and thus restoring the plaintext. Since only the receiver knows his own private key, the third party can not decrypt the information. It makes up the defect of the symmetric encryption algorithm. Combining the advantages and disadvantages of DES and RSA, to ensure the security and speed of information encryption and decryption, a combination of both methods are used, i.e, DES key is encrypted with RSA based on DES encrypting plaintext data.

2.VPN Technology. VPN technology is through the confusion of the public network to establish a temporary and safe connection channel. VPN technology is one of the main technology 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. Therefore, creating a temporary, secure, stable virtual private network channel in the public network to achieve internetworking between local cotton warehouse and central data center can make the data transmission fast and secure.

Security gateway is an organic fusion of various technologies, itself still has VPN functions, and establishes a VPN tunnel to the database server. Security gateway has an important and unique protective role, and itself has functions of firewall, antivirus, intrusion detection, user access active authentication and others. It also has a multi-network blocking function, that can only visit the protected network by 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 cotton warehouse and the external network connects to public network, and the user is isolated from the protected network by gateway, Security gateway deployment diagram is shown in Figure 2. The user and client initiate a request to create a tunnel and then create it, in 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, decision whether to allow the user (user or client) access or not is made according to the access control, only the user (client) that gained the 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.

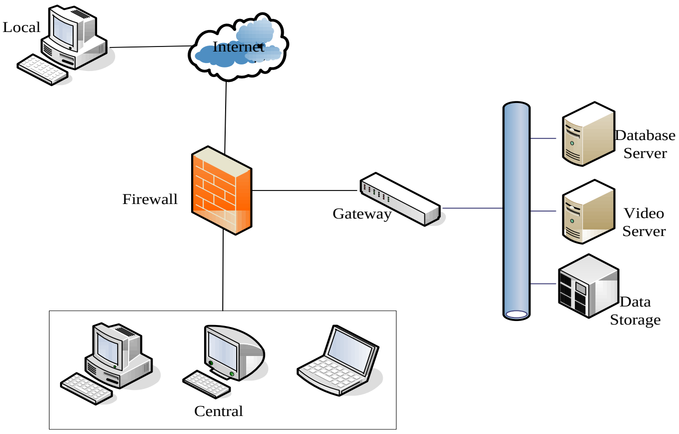

Fig.2 Security Gateway Deployment Diagram

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

1. Security desktop. In order to prevent the illegal user's access, users (clients) install desktop security software on the computer. When users are using client to access security desktop software, they need to pass strict user authentication. When making the identity authentication, the user needs to use the USB Key to verify the identity of the client, after gaining access to the corresponding operation[4]. Such as they must insert USBKEY to login system, the accession number and the password must match, only pass the verification, authorized users can access to information.

In the applications process of security desktop, user terminal without leaving any data, the data is stored in the background disk array, users only need to consider protecting background disk to prevent information leakage. So, using the algorithm of data encryption storage, the front-end system platform may cause information leakage probability will be greatly reduced.

2. Hierarchical access. Statistics, at present enterprise information leaks at least 60% from desktop security management within the enterprise. Therefore, facing all kinds of users, enterprise internal desktop security management problem has become one of the biggest problems faced by information security. Access permissions are associated with the role, and the role is associated with the users, so as to realize the logical separation between users and the access permissions [3]. Therefore, introducing the role as an intermediary. Rights management can define the various roles according to need, and set up the corresponding access permissions for the role. Due to the same jobs tend to be the same or similar business, according to their job and responsibilities assigned to different roles, such as system administrators and ordinary users, for the average user, the user management feature is not visible. For the local user, System at the central level of some of the pages are not visible.

A user can be assigned to multiple roles, a role has the right to perform multiple functions, a function can be achieved by multiple web pages. After entering system, different users see different function menu. so as to realize the logical separation between user and permission, to ensure that resources are not being illegally accessed and used, to ensure the security of the system.

Security Policy Analysis

In short, for the security problems that exist in the whole big system, from the aspects of hardware, for some smart devices lack of security problems ,through secondary development for the temperature or humidity sensors and cameras 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, to prevent the use of terminal network intrusion. For local cotton storehouse to the central data center to connect to the Internet is not protected in the process of transmission, using VPN technology to ensure that the data is not being attacked or tampered by a third party during the process of transmission. In the monitoring center computer terminals on the control and operation of security protection measures, fixed in the center of the two levels of monitoring security desktop software installed on the computer terminal, to improve the data security of terminal equipment. From the aspects of software, Data storage using both DES and RSA encryption of combining the methods of data encryption, to ensure the safety of data storage and transmission. For cotton library staff access to information access to the implementation of grading, to ensure access to the different roles of different resources. In this way, the maximum security of information transmission is achieved with minimum investment without changing the structure of the network.

Conclusion

This paper analyzed the security problems from perception layer to application layer of IoT, and put forward countermeasures to the security problem of every level, to prevent kinds of hackers, viruses, Trojan and holes respectively attacking on perception layer, transporting layer and application layer. However, security problem of IoT system is not a simple technical problem, it not only needs the safety awareness of developers and users with higher requirements, but also requires a combination of strict and scientific management, information security hidden danger to the whole Internet system to a minimum.

Acknowledgments

The research work was supported by 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 [D]: Beijing University of Posts and Telecommunications,2013

[2] Xu Wei. A Comparative Study of Desktop Terminal Security Management Technology [J]. Financial Electronic,2013,10:69-71.

[3] Long Qin, Liu Peng, Pan Aimin. Research and implementation of an extended administrative role-based access control modle[J].Research and development of the computer,2005,42(5):868~876.

[4] Wang Tao. The Design and Implementation of Remote Authentication System Based on USB Key [D]. Wuhan University of Science and Technology,2012.

[5] Su Kaiyuan. Research and implementation of the encryption algorithm[D]. Nanjing University of Posts and Telecommunications,2012.

[6] Li Anzhi, Cui Wei, Xu Yonghong. A authority controlling scheme in W eb accessing based on role[J]. Computer and information technology 6:4-6+46.

[7] Xia Shuhua. Research on data security transmission technology based on DES and RSA encryption algorithm [J]. Manufacturing Automation,2011,02:180-182.

[8] Wang Yan. Research on key technologies of information transmission for IoT control system [D].Northeast Forestry University,2012.

[9] Ma Qing. Research on Information Security Technology of IoT[J]. Computer and Network,2013,16:59-61.

[10]Hong Ren. Introduction to the Internet of things security issues and measures [J]. Computer CD Software and Application, 2012 (13) : 54-55.

[11] Liu Junbin, Wang Yong. Application of multi-campus network based on MPLS VPN[J].Value engineering,2014,03:188-190.

[12] Sun Lifei. Research on the campus network based on VPN technology[J]. Information and communication,2014,01:103-104.

[13] M.E.Hellman,"DES will be totally insecure within ten years". IEEE Spectrum,Vol.16,No7, pp32-39, July 1979

[14] Rivest R L, Shamir A, Adleman L.A method for obtaining digital signatures and public key cryptosystems[J]. Communications of the ACM,1978,21(2):120-126.

[15] Luigi Atzori, Antonio Iera, Giacomo Morabito. The Internet of Things: A survey [J]. Computer Networks, Volume 54, Issue 15, 28 October 2010, Pages 2787-2805.