The Study of Data Security Transmission in Chain Businesses

Pingping Dong
School of Information
Beijing WuZi University
Beijing China
E-mail: dpp1965@126.com

Jian Guo
School of Information
Beijing WuZi University
Beijing China
E-mail: guojian760118@163.com

***Abstract*—this text analyses the development of SMES and a new generation of chain enterprise management information system requirements for network data transmission. It mainly focuses on research how to ensure the important data transmission security between each branches and head office with present net security technology and encryption means including the analysis-design and implementation of data securely transmission. First, in part of data security transmission, the insecurity factor existing in current Internet are analyzed in detail and confirm how to ensure the safety of network data transmission on the analyzing conclusion. The second part is establishing the concrete implementation plan of network data transmission using XML technology and AES encryption technology and data security and RSA production safety signature means to realize network data safety transmission.**

Keywords-data;transmitting;encryption;decryption;chains business

I. INTRODUCTION

At present, the appliances distribution channels is in the period from old to new commercial form in China. The household appliance manufacturing enterprises also respond quickly to the development. The large sales channel has gradually shifted from independent agents to distribution companies and the home appliance chain enterprises have become the mainstream of the appliance sales.

The original management model of chain of appliance business is relatively independent of each branch and the warehouse is separated by city, using the monthly or quarterly summary report of the stocktaking query to the Corporation. The Corporation can grasp the sales and the warehousing of all the branches by analysis of the statements of the various branches and make the marketing plan of the next phase. The drawbacks of the pattern become increasingly clear with the continues expanding of sales scope and the development of information technology, that specific performance:

1）As home appliances market competition, changing market, in order to seize sales opportunities, you need to keep abreast of market conditions and store operations data, timely analyses the data of corporate for senior leadership decision-making. However, current management and information systems obviously can not meet the requirements.

2）According to their business operations and their operational characteristics, most of the chain distributors require headquarters and remote chain store warehouse, logistics, cash register systems and other business activities, information, and can take a real-time statistic to store the goods of each specific data.

3）The original system can not meet the pace of development of information technology. In terms of hardware and related system software is about to face the incompatibilities the original system required. With the increasing of branches number, the original data communications need to be improved in the data exchange frequency in order to get the market requirements at time.

4）The function of the applications needs to be adjusted and added.On the other hand a large number of advanced concepts and methods business process management must be introduced with the development of the company.

According to the development of chain enterprises the new generation of chain information systems are going to be a common feature on the Internet that enables instant communication via the Internet, data exchange function, which requires the new system to improve network data security encryption transmission technology, transmission of data in the public network can be effective against viruses and Trojans from network attacks and prevent hackers stealing important data on the enterprise, ensuring the security of corporate data transmission, accurate and complete.

II. SYSTEMATIC ANALYSIS OF CHAIN STORES

Invoicing system of chain stores are used to record their normal business. From inventory data as a starting point, purchase and sales and other business activities will result in daily changes in store inventory, which can directly reflect changes in the number of product sales, and reflect the home appliance sales trend in a period time.

Detailed records of chain stores business activities and help the branch managers to manage better the principal activities of the branch. Through the analysis of date sales data the managers can understand that which product has a good sales prospect in the current time and can understand the work performance of employees in the near future.

Published by Atlantis Press, Paris, France.

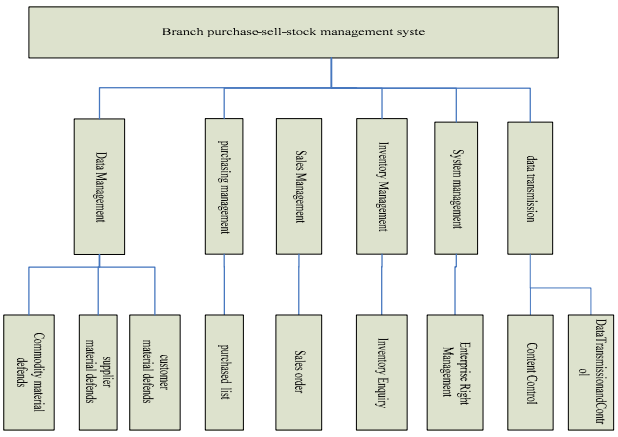

Figure 1. branches Invoicing system architecture

Sales are the main economic activities of business in each branch and the sales management is the core business management of every branch.Sales management includes the sales of goods, customer returns, sales return records the current record documents query.

The branch makes the purchasing strategy after analyzing the situation and inventory data of themselves. Purchasing depends on product sales prospects and current inventory status.The Geological position of each branch decides they have different suppliers.The purchasing management module should realize that the branch can manage the purchasing which is an important procurement activities.

Inventory management function is clear, including inventory information, inventory, reported profit loss report, the lower limit, lower limit alarm on inventory, historical query.

This article only discusses the analysis and implementation of data transferring between branches and headquarters.

III. ANALYSIS OF THE DATA TRANSMISSION SECURITY

A. The Purpose of Secure Data Transmission

The purpose of secure data transmission is to ensure that corporate business critical data safe through the Internet, not only to ensure that the needs of normal business activities of enterprises, but also to ensure data security and data accuracy and integrity.

With the development of large-scale enterprise management software and its more and more widely application the enterprise data platform involves the LAN and WAN and Internet etc.The business-critical data stored in various types of systems is also growing bigger and bigger. Many data need to be saved more than tens of year's even permanent preservation. So the key business data is the lifeline of enterprises and valuable resources and the data security is increasingly prominent. On one hand we should guarantee the physical network clear, for the enterprise data is transmitted through the public network and the Physical network hardware malfunction will produce a profound impact on enterprise data. On the other hand we should prevent hackers intercept data. Although today's network development tends to actively and favorable aspects but there are also some Illegal computer enthusiasts to attack and destroy our data transmitted in the network. In order to ensure the security of corporate data we must take the encrypted data and signature verification and identity authentication.

B. Data Transmission Security Analysis

In the chain sales systems the data exchanges between branches and head office are all through the network and the network system architecture layout has become one of the key steps. How to safely and accurately transfer the data is the core of the problem. Its solutions are in mainly two ways, and the first is setting up a virtual private network using VPN and the second is transmission of data to the head office database through the public network real-time.

Here we focus on the second transmission that the data flow handled safety is transmitted through the public network (that is Internet). The branch system download the important data to be transferred from the independent database in branch to the server's memory and generate the corresponding data file to be transferred. After that the file is encrypted and is translated type in order to make it to be safety I / O data stream, and is temporarily stored in the memory of database server for delivery. Data security transmission model is shown in figure 2.

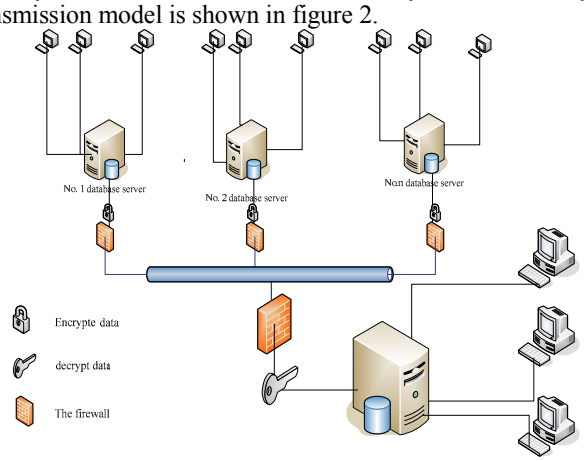

Figure 2. Chain home appliance enterprise system network structure

After the data flow has been encrypted the branch system send the data transfer request to head office server through the public network.The head office server validate the request and send receiving data response. Both the system controls the firewall to open the specified port to establish a secure channel for the encrypted data transmission. Data flow is transmitted to the memory of head office server through the external network. When the communication ended, the branch server sends ending communication signals .The head office server receives close request and shut down secure communications .The two sides close the communications and the security information channel is disconnected.

After the security information channel is closed the server start to process the received encrypted data stream, that is, implement decryption process contrary to encryption behavior. The process is accordance with the encryption process sequence. For example if the encrypted order is compression and type conversion type and encryption the decrypted order must be decryption and reversed-phase type conversion and uncompress, until is converted into ADO.Net which Dataset can be operated and the data stream has been restored. After the decryption process finished the DBMS in head office server add the restored dataflow to database according to a fixed data manipulation.

After the dataflow transmission is finished the branch invoicing system clear away the temporary data table and encrypted data flow copy resident in memory that will make the server has no redundant data storage in memory and guarantee the database server security and clean.

IV. DESIGNED AND IMPLEMENTED OF DATA SECURE TRANSMISSION

According to the design and analysis result, data transmission should ensure the continuity and integrity of data. Because the data is exchanged through the public network, the physical condition of the public network played a key role in the process of data transmission. Once the public network is not smooth the data will be lost or abnormal .So we propose a strategy first preserve before transmission. At first the data to be transferred is preserved as XML data file in the local sender and the relative information is stored in the database.

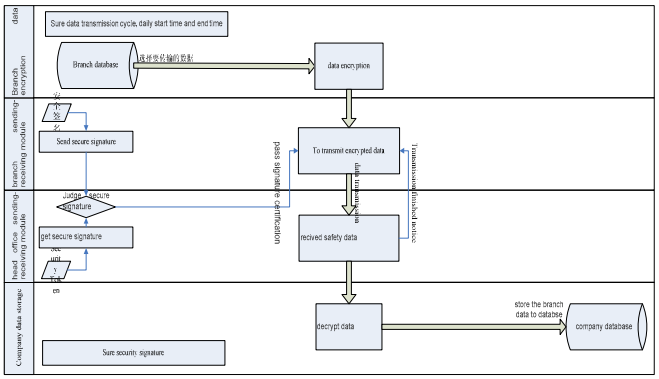

Figure 3. secure data transmission transaction flow diagram

A. XML data Stream Encryption Design

For the reality of enterprise data and data security, the transmission data is encrypted with symmetrical encryption algorithm. The advantages of the algorithm are that it can encrypt a large number of data in short time and the encryption algorithms are secure.

Symmetric encryption algorithm is applied earlier and mature. In symmetric encryption algorithm, the data sender handle the plaintext (raw data) and encryption key with a specially encryption algorithm and sent it as a complex encrypted cipher text. Data receiver receives the cipher text and need to use the same encryption key and algorithm to decrypt the cipher text. And put it back into readable plaintext.

The scheme uses AES symmetric encryption algorithm to encrypt XML data. AES is grouping keys and its algorithm needs 128-bit input data, the length of key cryptogram is also 128-bit. Algorithm requires expend key Expandedkey (i) that has the same length as the input packet in each round. As the length of the encryption key K external inputted is limited , so a key extensions is needed to extend the external key K into a longer bit strings in the algorithm to generate the encryption and decryption key each round.

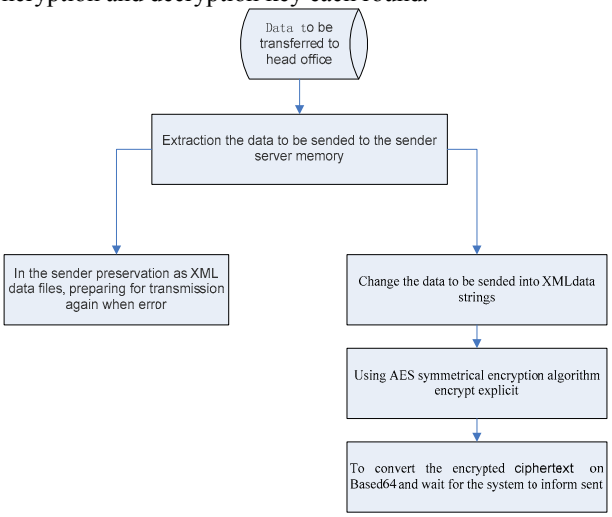

Figure 4. AES encryption of XML data flow diagram

B. Secure Signature Design

The secure signature uses the RSA encryption algorithm agreed by two sides. RSA is asymmetric encryption algorithm, which is characterized by public encryption key and respective decryption key. Asymmetric encryption algorithm is more complex than symmetric encryption algorithm and not suitable for extensive data encryption.

The basic principle of asymmetric encryption algorithm, if the sender wants to send the encrypted information only prepared for receive side the sender must first know the public key opposite side, and then encrypt the original files with their own public key; The head office server decrypt the received cipher text with their own private key. Clearly, the asymmetric encryption algorithm need the receiver must sent his public key generated randomly early to sender and retained the private key by itself before communication. For asymmetric algorithms has two keys it is especially suitable for data encryption in a distributed system.RSA and DSA propounded by the American National Standards Institutes are Widely used asymmetric encryption algorithm.

First the branch makes a convention with the head office about the singed content. The system provides modifying the signature function. Two sides save the convention signature information as secure encrypted XML file, so that the branch can send the signature content to head office system for verification before sending data.

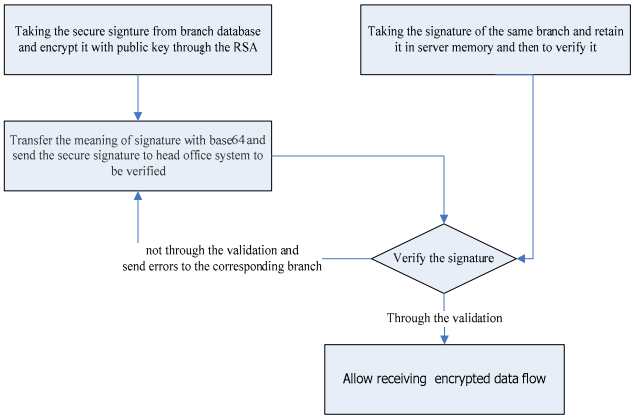

Figure 5. security signatures flow chart

The system will encrypt the signature string entered by system administrator with RAS encryption algorithm and saved in the XML file so that it is difficult for someone not knowing RSA decrypting key to decipher the signature content. The basic content of the security signature should include the branch number and safety signature. In every sending data cycle the security signature is taken from the system XML file and is transferred meaning with BASE64.So even if the security signature was intercepted, it is still quite difficult to decipher.

From the Angle of secure management the frequent replacement of encryption and decryption key of security signature is a necessary approach. Even most perfect technology still is likely intercepted and cracked, so only periodic replacement of encryption and decryption key can effectively prevent the RSA encrypted signature from being deciphered.

Security signatures is sent to the Server System in the head office, Server System take out the signature from their own security system and verify it with the branch signature. If the signatures are identical the head office server sends instructions agreeing to receive the encrypted data flow from the specified branch.

C. Set Transmission Cycle

Transmission cycle setting module is designed specifically for the branch, the module is responsible for setting the cycle of sending encryption data that is the interval of sending data request to the head office system. The cycle determines the frequency for the branch system visit the head office system. The cycle is designed according to the business hours of the branch and the number of branch owned by the enterprises, the server capacity of company's system, as well as the specific business needs of the enterprise .Because the cycle is influenced by the enterprise business so it is the constantly changing. The system should have the function of modify manually cycle.

D. Head Office Data Summarizing Systems

Data receiving module mainly is to respond to the data receiving request from branch system and receive security data encrypted from the branch.

Consideration of data safety for the relationship between the head office and branch is 1 to many all the security certification information should be stored in SQL Server database not XML file. The head office receives the data from branch and decrypt it on RSA deciphers process and converts it into a valid XML data stream. Then the XML data is transmitted to a temporary Dataset in the server's memory .The head office system updates corresponding branch inventory data according to the Dataset. The head office system updates the inventory data table daily at regular time on inventory data information transmitted from each branch to ensure that the total inventory data is generated the day before after every branch finished their business.

V. CONCLUSION

As the home appliance chain is in an increasingly competition, how to make the branch resources allocation more rational has become the top priority of each chain enterprise and it is also main business activities of enterprise. At the same time the data transmission security between the branch and the head office become one of the questions to be considered first. We must strengthen important data transmission safety on the network to prevent it from being intercepted, cracked, and damaged. The enterprises will make full use of Internet resources and reduce operating costs and improving the work efficiency.

ACKNOWLEDGMENT

This research was supported by Funding Project for Academic Human Resources Development in Institutions of Higher Learning Under the Jurisdiction of Beijing Municipality（PHR200906210）and Funding Project for Base Construction of Scientific Research of Beijing Municipal Commission of Education（WYJD200902）

REFERENCES

[1] James Huddleston a, Yang Hao translated, "C # Beginning Database "(2nd edition), Beijing: Tsinghua University Press, 2006.04.

[2] Ma Jun, Zheng Fengbin, Xia Shen Jiong, "C # web application of advanced into ", Beijing: People's Posts & Telecom Press, 2006.10.

[3] Simon Robinson, Christian Nagel.Professional, "C # (Third Edition)" . Published by Wiley Publishing, Inc, 2004.06.

[4] Gao Chuan. Proficient, " SQL - Structured Query Language Detailed" , Beijing: People's Posts & Telecom Press, 2007.03.

[5] Sa Shi Xuan, Wang Shan, "Database System", Beijing: Higher Education Press, 2002.02.

[6] Turley, Wood a, Ying Liu, "SQL Server 2005 in-depth development series - SQL Server 2005 Transact-SQL Programming Introduction to the classic", Beijing: Tsinghua University Press, 2007.02.