International Journal of Intelligent Information and Management Science
ISSN: 2307-0692, Volume 7, Issue 2, April, 2018

Research on Multi-user Privacy Data Security Verification Technology in the Process of E-commerce Transaction

Yan Zhang
School of Business, Northwest University of Politics and Law, Xi'an, 710063, China

Abstract: With the rapid development of modern Internet technology, e-commerce has become the main way for people to conduct business activities. However, due to the open nature of network transmission, the issue of user privacy data in the process of business transaction has always been an important constraint factor for the development of e-commerce. In this regard, this paper designs a multi-user privacy data security verification technology in the e-commerce transaction process. Through the central encryption module, the transaction data is encrypted with asymmetric key, and data ciphertext and security tokens are generated to achieve authentication, thereby protecting e-commerce information and user transaction information.

Keywords: E-commerce; Privacy data; Security verification; Encryption module

1. Introduction

The major security issues faced in modern e-commerce transaction include: invasion of secure transaction systems, eavesdropping of transaction information, falsification of user's personal information, fraud of transaction certificates and so on. The above security risks can be fundamentally divided into two categories: lower layer business transaction physical system security and business logic security. Physical system security mainly includes computer hardware network security in the process of e-commerce transaction. Business logic security mainly refers to transaction security during e-commerce transaction, involving the secure transmission of network information, information system firewalls and so on. The contents of the security work of e-commerce transaction mainly include ensuring the confidentiality, integrity, and irrevocability of information systems used by users during e-commerce transaction. Most of the traditional e-commerce transaction security protection is simply relying on the system firewall, which does not protect the user information itself and is easy to cause information leakage. Therefore, we must develop a new type of e-commerce user privacy data security verification technology, starting from the transaction user data, then carrying out ciphertext protection of transaction data through data encryption, and finally conducting verify the security token to get private data[1].

2. The Design of HC Data Encryption Module

The encryption of transaction data mainly uses information encryption algorithms designed in advance to generate private data in the state of plaintext as ciphertext of the information data, preventing illegal users from directly obtaining transaction data and ensuring the confidentiality of the transaction data. The related technology application of data encryption can largely solve the security problem of electronic transaction user's privacy data. The process of data encryption and decryption is shown in Figure 1.

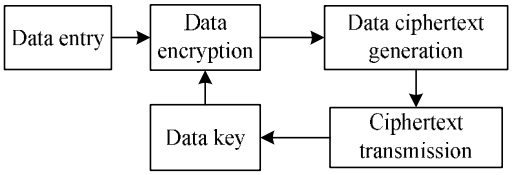

Figure 1. E-Commerce Data Encryption Steps.

The designed data encryption module uses the HC data encryption system as the core encryption area, generates the data key, encrypts the business transaction data in real time, and generates data token. In addition, on the basis of the fixed structure of the HC data encryption system, a dual mapping technique is added, two different linear quantities are programmed, and comparative key verification is performed to jointly constitute the transaction data encryption module [2].

2.1. The Generation of HC Data Ciphertext

The HC encryption system is the core encryption area of the entire encryption module. In addition to the conventional ciphertext generation for the privacy data of business users, the HC encryption system also has the function of self-generated and multi-layered distribution of

encryption keys. The system includes multiple root SKG files and a system SKG master file. After the business user data is entered, the system SKG master file can generate an encrypted domain file for the business user information, generate an information key according to the domain file identification code. After receiving the key of each layer, the domain SKG file can combine the original key generated by itself with the characteristics of the business user's personal transaction data information to generate information private key for the corresponding data domain point structure of each layer, that is the lower domain of each layer and finally return to the upper domain [3].

The overall security advantage of the HC data encryption system lies in the establishment of dual-line mappings and multiple forms of encryption of system SKG files and SKG files at each layer. There are four parts of the encryption algorithm for double SKG files: initialization encryption, key encryption, ciphertext generation. and security token generation. The function of each part is shown as follows:

Initialization encryption: The administrators of e-commerce transaction information database can enter a security parameter in advance in the data encryption module for setting up the largest information structure level, and generate the main key of public information parameter management through the initialization algorithm.

Key encryption: Database administrators output key ID parameters and establish data keys through the management IDs of e-commerce users at each level and the user keys of each level's business users.

Ciphertext generation: The encryption module encrypts the user information plaintext of the corresponding IDs and outputs ciphertext instructions by outputting the key ID parameters.

Security token generation: The security token is essentially a set of ciphertext structure codes. The data encryption module can generate a verification security token based on the specific digital information of the ciphertext and transmit it to the user of the e-commerce transaction for unlocking the ciphertext [4].

2.2. The Design of HC Dual-Line Encryption Mapping

In order to further improve the confidentiality of e-commerce transaction and the verification effect of security token, a dual-line mapping design is applied on the basis of the HC encryption module. The dual-line mapping is to conduct the P1 and P2 dual-line quantity mixing in the design of the encryption module, ie, P1 and P2 are two sets of line quantity keys for comparative keys verification. In the HC dual-line mapping, P1 and P2 are essentially two H-degree ciphertext data multiplicative groups. G-order is a stage of file management authority, its role is to generate source files.

When the business user's personal information data or transaction information data needs to be transmitted between network nodes, the HC encryption system can generate a personal information solution key corresponding to his identity level for each administrator of the encryption system. The decryption authority for each solution key is different because of the difference of levels. The solution key can be used to decrypt the personal data information files of each layer, so as to ensure the safety and integrity of the user's personal information data. In addition, system authentication and personal information transmission can be completed in the system locally, which not only improves the operating efficiency, but also increases the corresponding monitoring target.

3. The Design of Privacy Data Security Verification System of The HC Business User

The privacy data security verification system of the HC business user is based on the HC data encryption module design and identity layering idea. It is designed for the privacy data security and integrity of transaction users and is used in the privacy data security verification system in the e-commerce transaction process. The main work flow chart is shown in Figure 2.

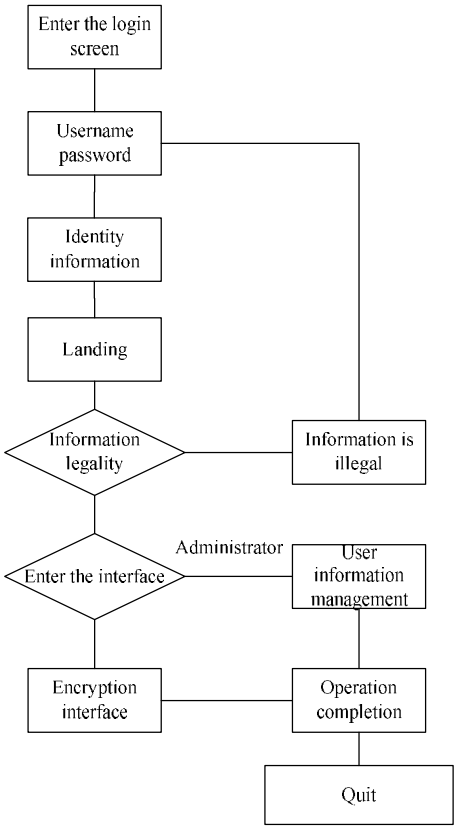

Figure 2. Work Flow Chart.

The entire verification system uses JAVA language programming, combined with HC data encryption module and ciphertext key generation to achieve the work flow. The system has four main functional modules: user login module, security verification management module, personal information data encryption and decryption module [5].

3.1. The Function Design of User Login Module

The user login module mainly exists as a system login interface. Through different security tokens and account information, the system administrator and user identity can be automatically distinguished. The operator uses a different identity ID to log in and the operation interface is different. In addition, this user login module has an account lock function. If the number of account password errors is too many, the account will be locked, which ensures the security of the business information to some extent.

3.2. The Design of Security Verification Management Module

The main function of the security verification management module is to allow administrators or business users to perform security verification based on the cryptographic tokens they obtain and manage their business information hierarchically. Through user-related, it is possible to add, delete, classify, classify structure information, search for information, modify information, and carry out other operations on various types of information.

3.3. Personal information data encryption and decryption module

The main function of the file encryption and decryption module is to generate an identity key verification system corresponding to the user login information returned from the login page. Each key domain information is connected with the database, which is the user's most important identity certificate, and the user needs to carry out data verification by his own security token. The function of this module is mainly achieved through the HC encryption system.

When the system receives the user's verification instruction for the related business document information, the system will independently verify the identity of the decryption person. Through the comparison of the file name and the security token, it can determine whether the decryption person has the decryption authority of the relevant file data. If the person has can the authority, it can be decrypted, the data ciphertext will be generated as plaintext, otherwise it is not allowed to be decrypted. The specific process is shown in Figure 3.

4. The Privacy Data Security Verification System of The HC Business User

4.1. Encryption Algorithm Analysis Code

The HC data encryption module includes four core algorithms: initial encryption, key encryption, ciphertext generation, and security token generation. Its part of the algorithm code is shown below.

A lgor}thsssm Setup
IuputArry})
0 utput such as aramsdfewess, msk)
9de-GdWg
G2}g3}h},. ., h- G
Params}}g,g,,gz,g3,h},..., hi),msk~gz
To rn plus dfewerarams, msaioik) A lgor}sqethm K eyG eawn

4.2. The Design of The Encryption System Packet

In order to realize the system functions of some functional modules, the entire security verification system designs four core data packets for the individual through the interface. The functions corresponding to each core data packet are shown in Table 1.

Table 1. Packet Function Table.

Packet name	Function
.JAVA.datebag1	Data encryption and security token generation
JAVA.datebag2	Encryption system operation management
JAVA.datebag3	System login interface
JAVA.datebag4	Module corresponding to the user interface

5. Conclusion

The HC business user privacy data security verification system is designed based on the HC data encryption module, and it is the security system used to protect the e-commerce transaction information data. The system can not only satisfy the confidentiality of users' daily data transmission, but also the complete ciphertext generation and security token verification functions greatly improve the security of personal e-commerce transaction information.

References

[1] Qian Min, Jiang Yu. The Relationship between Data Mining and Privacy in E-commerce [J]. China Science and Technology Information, 2016, 8 (8): 135-136.

[2] Tian Haibo, He Jiejie, Fu Liqing. Agreement on Privacy Protection Fair Contract Based on Public Blockchain. [J]. Journal of Cryptologic Research, 2017, 4 (2): 187-198.

[3] Shi Wenbing, Hua Fengliang. Design of Buyer Privacy Protection Transaction Protocol Based on Third-party Payment Platform [J]. Network Security Technology and Application, 2016, 45 (1): 89-90.

[4] Wang Liming. Chen Tinggui, Sun Lan. Bidirectional Authentication Mobile Payment Algorithm Based on Transaction Authentication Mode in Mobile Advertising [J]. Journal of Jingmen Technical College, 2016, 31, 69 (4): 41-47.

[5] Zhang Peng. Study on Legal Protection of Consumers' Privacy Right in Online Trading [J]. Economy, 2016, 58 (1): 00191-00191.