Design and Implementation of B2C-based E-commerce Secure Payment System

Haohua Qing¹, Jiali zhang², Hong Cao³

¹Department of Economic And Trade, Guangzhou College of Technology and Business, Guangzhou, 510850, Guangdong, China
²Department of Computer Science and Engineering, Guangzhou College of Technology and Business, Guangzhou, 510850, Guangdong, China
³Guangzhou Modern Information Engineering College, Guangzhou, 510850, Guangdong, China

*Corresponding author E-mail: 13986536@sasu.edu.cn

Abstract. With the popularization and application of information network technology such as the Internet in various industries and even ordinary families, people have entered the information age based on the network, and the electronic commerce based on the Internet has also been developed rapidly in the world, and has become a new mode of modern business trade. In order to promote the development of electronic commerce in China, we should actively study and develop the corresponding electronic payment methods. Through the efforts in recent years, great progress has been made in the construction of financial electronics in China. Five national electronic fund transfer systems have been built. According to statistics, in recent years, the transaction volume of e-commerce in China has exceeded 4 trillion yuan, and the total transaction volume of e-commerce payments such as online payment of mobile phones on the Internet has exceeded trillion yuan.

Keywords: B2C, E-commerce, Secure Payment Systems, Information Network Technology

1. Introduction

The rapid development of e-commerce industry will bring unlimited opportunities to the banking industry. If the bank has a timely update in the technology of safe payment, it can meet the needs of the development of e-commerce, then the whole banking industry will be the biggest beneficiary of e-commerce and the lasting and powerful driving force of the e-commerce industry. Online payment system is the core of e-commerce, so the key of e-commerce is to provide a reliable, safe, convenient and practical online payment system.

Design and implementation of e-commerce security payment system based on B2C has attracted the interest of many experts and has been studied by many teams. Some teams, for example, have found that while NFC mobile payments can bring great convenience to people, there are many security threats and vulnerabilities. A complete NFC mobile payment transaction generally has four
participants: one is a mobile terminal with a security unit, which is generally held by consumer customers to complete the payment operation[1]; Second, the merchant's POS machine or other reading equipment acts as the processing terminal and provides transaction data to the trusted authentication platform as the initiator of the transaction; third, the TSM platform receives transaction information and confirms the integrity and validity of account and transaction information with the bank; and fourth, the banking system, mainly as a clearing system and account management system, settles transaction funds, withdraws fees from user accounts and transfers merchant accounts[2]. Some teams found that from the birth of mobile payment technology to now, the situation in our country generally started late in the initial stage, and the promotion was slow, which was mainly caused by two reasons: on the one hand, China's mobile terminal performance is weak, mobile Internet infrastructure is weak, restricting the development of mobile payment; on the other hand, due to the immature mobile payment industry chain, the interests of the ecological circle can not be agreed[3]. However, with the popularity of smart phones, the performance of domestic mobile phones in China has been in the forefront of the world, terminal problems are no longer a factor restricting the development of mobile payment, because mobile operators build a large-scale 4G network, signal and network speed are no longer restricted[4]. In recent years, China's mobile payment market has gradually matured due to joint payments, Internet companies such as Ali Tencent JingDong, mobile telecom Unicom and other operators and major mobile phone manufacturers[5]. For many consumers, mobile phones have been able to replace cash, bank cards, bus cards and so on, carrying is very convenient, the consumption process is more convenient, safe and simple, and because the use of mobile payment settlement to avoid cash settlement is not easy to change, do not distinguish counterfeit currency and other advantages, more and more people prefer to use mobile payment. At present, it can be said that China's mobile payment has been in the forefront of the world, as long as a mobile phone can achieve all aspects of daily life applications[6]. Other teams found that in the past 10 years, the development speed of China's telecommunications industry is amazing, and the development of users is geometric, but with the increase of the number of users and the intensification of competition, the traditional sources of income (such as network access fees, monthly rental fees, call fees, etc.), etc. In order to develop new sources of revenue and attract more users, the demand of telecom operators for special value-added services has been increasing and increasing over time. In order to seize the market opportunities, China Mobile Communications Group has taken the lead in developing new mobile e-commerce services[7]. Although their research results are very rich, but there are still some shortcomings.

This paper first proposes an efficient and secure online trading scheme of fusion SSL protocol to ensure the security of data during transmission. Secondly, some sensitive information is MD5 encrypted and stored in the database to ensure the security of data during storage. Finally, combined with the existing payment system, including Alipay payment system and Industrial Bank payment system, the department store shopping online payment system is implemented in PHPMSSQLServer part.

2. Method

2.1. Human Behavior Recognition Algorithm Based on 3DCNN

The derivative function derives the key from other entropy sources while maintaining the entropy of the input and is unidirectional. A key derivation is often used not only to generate a key, but also to use IV. At the same time, it must be understood that the strength of a KDF depends on the entropy of the encrypted information and the strength of the calculation of the function itself, because as a decipher, it is possible to guess the encrypted information, so it is very likely to calculate the derived key. The KDF used in this paper is based on the SHA-1 hash function, and the key K and initial vector IV are obtained by connecting the D1 and the D2, which are defined as follows[8]:

\[ D_i = SHA^{count}\left(D_{i-1}||keyData||salt\right) \]
Count is an integer, representing the difficulty of KDF function calculation, salt random bits are used to improve security, prevent precomputed dictionary attacks, || means a connection, D0 is empty, SHA11(data) is a simple SHA1(data), SHA12(data) is SHA1(data) and so on, keyData is defined as:

\[ keyData = SHA1(Password) \| ServiceKey \| UserName \]  

(2)

Among them, the user needs to encrypt or decrypt the unique identity of the security information, and the UserName is the unique user name of the user authentication service. Accordingly, in summary, the process of obtaining the key key and the initial vector is as follows:

\[ SHA1(Password) \| ServiceKey \rightarrow SHA1\text{-basedKDF} \rightarrow key \| IV \]  

(3)

2.2. Random Number Generator

The salt to be entered in the KDF mentioned above need to be generated by the random number generator, and in the random soft keyboard to be mentioned below, the random number generator is also needed to generate the key bits that determine the keyboard. The random generation method used here is the function java.security.In secure random class the algorithm uses an algorithm called SHA1PRNG, which is very similar to the algorithm used in the KDF, and the output of the random number is also obtained by D1 and D2 iteration. The Di is defined as follows[9]:

\[ D_i = SHA1(D_{i-1} \| seed) \]  

(4)

2.3. Settlement Phase

POS sign and encrypt transaction records and send settlement messages to TSM platforms as follows[10]:

\[ E_{PKTSM}(ID_{POS} \| E_{SKPOS}(U, R, h, s1, s2, price, Timestamp, H(m))) \]  

(5)

3. Experiment

3.1. Source of Experimental Data

The main research object of this paper is the bank of Hubei province. Secondly, by reviewing the existing research literature and related theories, the theoretical research model is put forward, and then the required data are collected by questionnaire. After data analysis, the research model is optimized. A total of 101 questionnaires were collected, 83 valid questionnaires and 81% effective.

3.2. Experimental Design

1. The briefly describes the online security payment system, deeply studies and discusses the various security technologies needed to realize online payment. 2. The SET protocol, SSL protocol and 3D security payment protocol are analyzed and studied in detail, their security vulnerabilities and shortcomings are found, and the advantages of SET protocol and SSL protocol are taken advantage of. The idea of strengthening the SSL protocol is put forward to solve the problem of data transmission security caused by the short length of symmetric key. Then the foreign e-commerce website protocol and its application are discussed, mainly used in foreign e-commerce websites. 4. Finally, the security prevention mechanism based on electronic transaction protocol, security prevention based on transmission layer, security prevention based on database and auxiliary security prevention are put forward. On this basis, the application process of online shopping system of department store is introduced. This paper mainly uses literature method, empirical analysis method and comparative analysis method.
4. Result

4.1. Analysis on the Statistics of the Overall Research Paper on E-commerce Payment
The statistics and investigation of research papers and papers on e-commerce payment are mainly based on several databases at home and abroad. E-commerce payment is not a highly recognized professional vocabulary. In practice and theory, there are many corresponding professional terms. The results show that the total number of e-commerce payment papers in China is 6 years, and the distribution of papers is shown in Table 1.

Table 1. Quantitative distribution of research papers on e-commerce payments in China

|                | 2015 | 2016 | 2017 | 2018 | 2019 | 2020 | Amount to  |
|----------------|------|------|------|------|------|------|-----------|
| E-commerce payments | 19   | 19   | 21   | 32   | 16   | 5    | 116       |
| Electronic money   | 408  | 319  | 232  | 290  | 262  | 110  | 1627      |
| Online payment     | 100  | 40   | 106  | 102  | 98   | 41   | 487       |
| On-line payment    | 593  | 293  | 330  | 456  | 412  | 206  | 2290      |
| Electronic payment | 449  | 297  | 344  | 694  | 645  | 325  | 2756      |
| Altogether         | 1569 | 968  | 1033 | 1574 | 1433 | 687  | 7276      |

In the six years listed in Table 1, the number of e-commerce payment papers reached a peak of 1569 five years ago, reflecting the high attention paid to new things. But since then, the number of papers per year has dropped sharply to more than half, to 1033 by 2017 and to 1574 by 2018. It can be seen from the Table that e-payment, online payment, e-money, online payment and e-commerce payment gradually decrease in the total number of papers, especially the number of papers paid to e-commerce is only 2%, which indicates that there is little systematic research on e-commerce payment.

4.2. Analysis of Autonomous Access Control Method
Nowadays, the general database management system provides independent access control, and the SQL standard is mainly realized by GRANT statements and REVOKE statements. In relational database systems, access control objects include data and database patterns. The main access rights are listed in Table 2 below.

Table 2. Relational database access rights

| object type | target          | operation type                                           |
|-------------|-----------------|----------------------------------------------------------|
| data base   | model           | CREATE SCHEMA                                            |
|             | basic list      | CREATE Table,ALTER Table                                 |
| model       | view            | CREATE VIEW                                              |
|             | index           | CREATE INDEX                                             |
| data        | basic Tables and views | SELECT,INSERT,UPDATE,DELETE,REFERENCES,REFERENCES ALL PRIVILEGES |
|             | property column | SELECT,INSERT,UPDATE,REFERENCES,REFERENCES ALL PRIVILEGES |

4.3. Analysis of Website Development and Online Banking
According to the online survey, there are 26 commercial banks in Hubei province, including 15 national commercial banks, 7 local commercial banks and 5 foreign banks. The article also investigates
the website construction and online banking of commercial banks in Hubei province, in which national commercial banks and foreign banks have credit cards, debit cards, stored value cards, and enterprise and government payment schemes with provincial branches, in the service to enterprises and governments, visa specifically targeting government services, while MasterCard focuses on the services of multinational corporations, whether portals and head offices carry out online banking business as the statistical basis, and whether local commercial banks have portals and online banking business as the statistical basis, as shown in Figure 1.

Figure 1. Construction of Hubei Commercial Bank website and development of online banking

4.4. Analysis of the Status of the Third Party Payment Platform

In recent years, with the increasing demand for online payment and the promotion of funds, China's third-party payment platform has also made unprecedented development. At present, China has more than 50 third-party payment platforms, providing different online payment services and products. In the first quarter of 2011, China's third-party payments reached 36.5 billion yuan, according to the report the company's transactions were 36.5 billion yuan, up 3.2 percent from a month earlier, up 102.6 percent from the same period last year. The specific market share of the company is shown in Figure 2.
As can be seen from Figure 2, payment dust occupies an absolute advantage, close to half of the market share, tenpay ranks second, accounting for 20.61%. The two companies have obvious leading advantages. Its success is largely supported by the strong business resources, technical background and brand strength of the group. In this regard, many non-independent third-party payment enterprises are difficult to catch up in a short time.

5. Conclusion
With the rapid development of economy and the continuous progress of computer technology, e-commerce not only provides a sustained impetus for economic development, but also brings convenience to people's lives. However, as an important part of e-commerce system, e-commerce secure payment system is becoming more and more prominent. This paper studies the security technology needed for electronic payment, according to the transaction process and security requirements, referring to various electronic payment security protocols and electronic payment models, using data encryption technology to authenticate the system, and gives an electronic commerce security payment system. The system is analyzed from the aspects of workflow and information format.

References
[1] Mohammadi M T , Mazinani S M , Nikooghadam M , et al. LSPP: Lightweight and Secure Payment Protocol for Dynamic Wireless Charging of Electric Vehicles in Vehicular Cloud[J]. IEEE Access, 2019, PP(99):1-1.
[2] Ojetunde B , Shibata N , Gao J . Secure Payment System Utilizing MANET for Disaster Areas[J]. IEEE Transactions on Systems, Man, and Cybernetics, 2019, 49(12):2651-2663.
[3] Beik N , Reddy P , Sylvester K W , et al. Andexanet Alfa (Andexxa) Formulary Review[J]. Critical pathways in cardiology, 2019, 18(2):66-71.
[4] Singh S , Bangalore S , Amutha S , et al. Face Recognition for Payment and Information Sharing[J]. International Journal on Recent and Innovation Trends in Computing and Communication, 2020, 8(4):06-08.
[5] Sakulyeva T N . The Maas system and its problems[J]. E-Management, 2019(2):30-37.
[6] Papadis N , Tassilias L . Blockchain-Based Payment Channel Networks: Challenges and Recent Advances[J]. IEEE Access, 2020, PP(99):1-1.
[7] Gruenkorn A . SPOTLIGHT[J]. Intelligent Transport, 2019, 3(1):22-23.
[8] Bocsi G T , Kang J , Kennedy A , et al. Developing Pathology Measures for the Quality Payment Program-Part I: A Quest for Meaningful Measures[J]. Archives of Pathology & Laboratory Medicine, 2020, 144(6):686-696.
[9] Chen A , Hieber P , Klein J K . TONUITY: A NOVEL INDIVIDUAL-ORIENTED
[7] RETIREMENT PLAN[J]. Astin bulletin, 2019, 49(1):5-30.

[10] Ghazali O, Leow C Y, Qaiser S, et al. Cloud-Based Global Online Marketplaces Review on Trust and Security[J]. International Journal of Interactive Mobile Technologies (iJIM), 2019, 13(4):96.