ISSN 2616-5775 Vol. 6, Issue 7: 188-192, DOI: 10.25236/AJCIS.2023.060725

Design of Electronic Commerce Secure Payment System Based on TOTP Algorithm

Li Sisi

Department of Information Engineering, Guangzhou Huashang Vocational College, Guangzhou, Guangdong, 511300, China
sisilee@gzhsvc.edu.cn

Abstract: *Due to the extended service time and slow payment network speed of existing e-commerce secure payment systems, the design of an e-commerce secure payment system based on the TOTP algorithm is studied. In terms of system hardware design, the card reader is connected to the POS machine and FRID for high and low frequency signal transmission, and the power module and RFID module chip are designed. In terms of system software design, the TOTP algorithm is used to generate passwords, which are fused with timestamps and converted into dynamic payment keys. The buyer and seller complete the payment operation by comparing and verifying each other's payment keys. The system extracts buyer feature values, classifies buyer consumption behavior, authenticates identity, and matches rules for risk assessment. The test results show that the service latency of the system using the design method in this article is within 0.3s, and the payment network speed is above 30MB/s, which meets the expected goals and achieves good application of the e-commerce secure payment system.*

Keywords: *TOTP algorithm; Electronic Commerce; Payment; System design*

1. Introduction

With the rapid development of modern society, e-commerce has been applied by the public because of its convenience. In the face of massive mobile payment participants, their privacy information should be strictly encrypted and stored. Not only the mobile terminal, but also the service provider should design a highly secure payment system to complete the transaction. Devices with high protection and security factor should be added in the storage process of payment information, and transmitted data should be encrypted [1]. It is not saved when the ciphertext plaintext is to be operated legally. During the payment process, sensitive data is usually stored in ciphertext to prevent attackers from obtaining it through attacks and eavesdropping, ensuring secure and complete transmission of effective information. A confirmation mechanism is added into the communication protocol to ensure that the communication process is not intercepted or to suppress signal interference [2].Realize encrypted transmission of communication data and protocol security through the security level of the payment system. Due to the presence of many participants in the mobile payment process, the existing payment systems do not attach high importance to the security issues of mobile payments in the e-commerce payment process, and do not provide a detailed division of specific communication data formats. Therefore, their feasibility in practical applications is relatively low. Enabling attackers to quickly steal buyer information and tamper with the buyer's private data at will. If the tampered data is transmitted to both receiving and sending parties, causing them to fail to detect it in a timely manner during the transaction process, it will result in serious property losses and very serious consequences. Therefore, at present, the e-commerce secure payment system is the research object, and the TOTP algorithm is used to test and analyze based on the actual situation

2. Payment system hardware design

The hardware design of electronic commerce secure payment system consists of three parts. Card reader is mainly used for high and low frequency signal transmission, and through the serial port connected to POS machine, RFID signal parsing.

ISSN 2616-5775 Vol. 6, Issue 7: 188-192, DOI: 10.25236/AJCIS.2023.060725

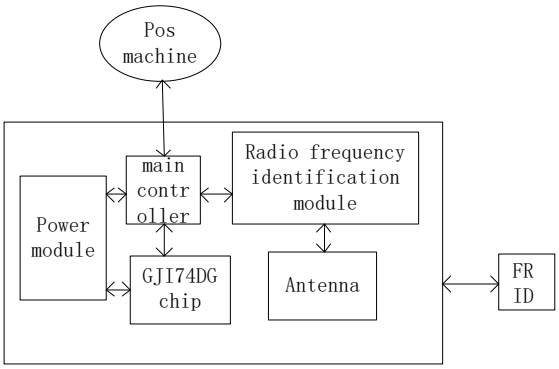

Figure 1: Hardware design diagram of the card reader

In the card reader, the power module powers up different positions inside the card reader in real-time. At the same time, control the power supply mode of the card reader, use DC and USB to transfer+3V power supply, and combine it with a level conversion chip to generate a 3.5V input voltage and transmit it to the remaining modules. The main controller module is the key module of the card reader, which connects the card reader to the POS machine by transmitting corresponding data [3]. The main controller module is responsible for controlling different modules and preventing detection conflicts during initialization.GJI74DG chip is used to series a variety of communication interfaces such as USB interface, SPI interface, etc. Built-in oscillation controller and PPL, access crystal, complete key management, data signature and buyer authentication. At the same time, low power consumption is supported, and the power consumption is 120mV. The radio frequency identification module uses the open 3.6GHz frequency band, with 26 channels for choice, the channel switching time is short, can achieve multi-frequency communication and frequency-hopping communication. The size of the RF channel is 3.6G, and the width is 2MHz.

3. Payment system software design

3.1 TOTP algorithm key dynamic payment

Set a dynamic QR code for dynamic payment, which can achieve core control in a secure cloud payment system. When transactions occur, timely generation of payment keys ensures payment behavior and security. Overall, it is necessary to encrypt the provided order information on time in both directions, and the buyer also needs to provide their payment key. Only after obtaining the complete cloud key decryption authentication can secure payment be achieved [4]. When making secure payments, it is necessary to continuously generate payment QR codes. According to the buyer's payment request, a dynamic payment QR code is generated in a short period of time and updated once within a certain period of time to ensure real-time use of the QR code, and this process continues until the payment is completed.In the process of transaction, the two-dimensional code received by different buyers is independently existing in the secure payment system. After the secure payment system receives the seller's order information, the authentication begins in real time according to the buyer's payment key. It is used to standardize the validity period of the payment key. TOTP algorithm is used to generate a 12-bit dynamic password, and then the password is combined with the time stamp to form a string. Hashing algorithm is used to transform the string into a dynamic payment key. Set the key string as g and the time stamp as D, and the formula for calculating the time stamp is as follows:

$$D = \frac{(T - T_1)}{F} \tag{1}$$

In the formula, T represents the current timestamp; T is 0; F is the time step. In general, $F = 30$. By using hash algorithm, the timestamp and the key string are encrypted, thus generating the corresponding key string. Then, the last 8 digits are extracted from the sorted bytes, which indicates both the index and the offset of the encrypted string. According to the offset indicated by the index, the corresponding number of bytes is calculated and combined to form an integer. Finally, the last 8 bits are extracted from the integer, converted into a string and returned. This process is to generate a part of the payment key to ensure the security of payment behavior. Due to the dynamic characteristics of TOTP, the buyer generates the corresponding password through the TOTP algorithm and converts it into a

ISSN 2616-5775 Vol. 6, Issue 7: 188-192, DOI: 10.25236/AJCIS.2023.060725

dynamic payment key [5].After receiving the order information, the secure payment system retrieves the order information that has not been paid, forms the payment key, and compares it with the payment key uploaded by the seller. If the key verification is successful, the specific amount of money paid by the buyer will be deducted after information processing and passed to the seller. If the key verification fails, the payment page is returned with the reason why the transaction failed.

3.2 Assess the degree of payment risk

After the seller receives the payment request, the secure payment system will conduct a risk assessment on it. By collecting buyers' personal information and consumption preferences, we can determine their consumption characteristics and record the data of each consumption. Based on these data, the security payment application is evaluated. In the transaction risk evaluation, the calculation formula of the prime Bayesian algorithm can be used to calculate the risk probability of the transaction, so as to judge whether there is potential risk or fraud in the transaction. The calculation formula of the prime Bayesian algorithm is:

$$A(W \mid R) = \frac{A(R \mid W)A(W)}{A(R)} \tag{2}$$

In the formula: W represents category; R is the data waiting for classification. Create set $T = \{t_1, t_2, ..., t_n\}$ of items to be classified, where t_n is the corresponding attribute feature. Continuous polynomial calculation of $A(w,r)$ [6]. If the existence of $A(w,r) = \max(A(w,r))$ is true, then r can be classified into class w.Conduct a security assessment on the behavioral characteristics reflected in different dimensions of data, set the payment time as N, payment term as U, payment quantity as x, seller information as b, and product name as z, and the set to be counted is $R = \{N, U, x, b, z\}$. Compare the normal value $A(yes)$ of $A(w,r)$ with the outlier $A(no)$. If the normal value is large, it is determined as normal payment.From the sample data of different attributes of the transaction, the transaction characteristic data is extracted, and the buyer's consumption style is marked and counted. If the secure payment system determines that it does not conform to the buyer's consumption habits, it will carefully verify the buyer's identity. If yes, the system matches the security rules. In the matching process, the specific rules can be customized, mainly for the buyer's payment price, the specific time of consumption and the city. When the buyer's identity is verified, the corresponding buyer's identity is generated. The identity is sent to the paying buyer's client. After the buyer logs in the system, he/she performs related operations under the identified conditions to make secure payment.

4. Test and analysis

To test the stability of the e-commerce secure payment system, three testing groups were set up, with the experimental group using the system designed in this article as the experimental group. The group using the traditional system is the control group. Set the total amount of resources during the payment process to 5500GB and divide it into 20 payments, uploading the payment data to the system. The data obtained through each payment is 150GB. Based on the actual transaction situation on site, set the number of servers to 3 and build a virtual server cluster. The storage space of different servers varies, with a minimum of 8GB and a maximum of 128GB.After the payment data is uploaded to the system, 500 buyers are selected to use the system simultaneously and send a payment service request to the system every 15s for one hour. In the experiment, the service response delay time of the system is taken as the test index. When the number of requests is 800, the maximum service delay time of the system is 0.3s. When the time for the buyer to send the service request to the system is set to start, the system displays the payment success and accepts the task result.

Time testing software OJHF is used to test the response delay of different systems. When the number of payment service requests is 100-800, the corresponding delay data of the three groups will be tested. The service delay results of the secure payment system are shown in Table 1:

It can be seen from the test results that, with the increasing number of requests, the delay of the two control groups is large, exceeding the expected target and failing to achieve good application. In the experimental group, the service delay is within 0.3s, and when the number of requests is 800, the delay

ISSN 2616-5775 Vol. 6, Issue 7: 188-192, DOI: 10.25236/AJCIS.2023.060725

is only 0.26s. It indicates that the system service response performance has good stability, is within the controllable range, and meets the expected objectives.

Table 1: Service delay result of secure payment system

Request quantity/piece	Experimental group	Control group 1	Control group 2
100	0.05	1.31	1.51
200	0.08	1.59	1.68
300	0.15	1.69	1.88
400	0.19	1.72	1.97
500	0.21	1.83	2.24
600	0.23	2.19	2.64
700	0.25	2.36	2.98
800	0.26	2.77	3.32

In order to further test the practicability of the payment system, the payment network speed of the system is used as the test index for comparative test, and the test results are shown in Figure 2 below.

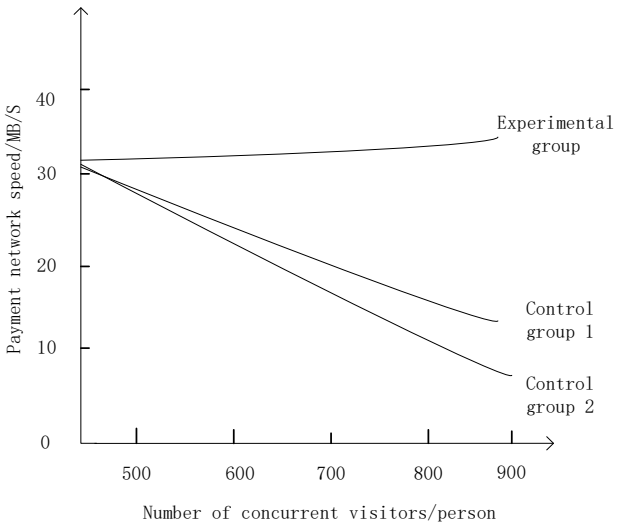

Figure 2: Network speed results during payment

The experimental results show that when the number of concurrent visitors reaches 900, the payment network speed of the two control groups drops to below 20MB/s. When the number of online payers exceeds the system's own load, it is very easy to cause network interruption and payment failure. Compared with the control group, the payment network of the experimental group was relatively stable, with a small improvement when the number of concurrent visitors was 800-900. An increase in the number of concurrent users will not slow down payment speeds. In the actual payment process, the system application effect is good, improve the network load rate, make the payment speed maintain a high level, achieve the expected goal. To sum up, the secure payment system designed by the method in this paper has good stability and applicability, and can provide buyers with high-quality payment services.

5. Conclusion

This study starts with secure payment and deeply analyzes the relevant issues of e-commerce payment, designing an e-commerce secure payment system based on the TOTP algorithm. To promote the good development of e-commerce payment security issues, a real-time payment system with high security is constructed, and TOTP algorithm is used for synchronous design according to corresponding design requirements. Organize and archive key data during the payment process to improve data confidentiality and facilitate the establishment and optimization of e-commerce systems.However, the method in this paper still has some shortcomings, such as imperfect analysis and selection of main samples and payment key setting. In the future, the calculation should be more perfect, through the continuous optimization of server storage space, coordination of resources and rational synchronization of methods, improve the service level of e-commerce system, solve various emergencies in the

ISSN 2616-5775 Vol. 6, Issue 7: 188-192, DOI: 10.25236/AJCIS.2023.060725

payment process, and realize the design of e-commerce security payment system based on TOTP algorithm.

References

[1] Yang Yifan. Development of Mobile Cloud Secure Payment System Based on TOTP Algorithm [J]. Microcomputer Applications, 2022, 38(05):188-191.
[2] Chen Zhigang, Cui Yanzheng. Design and practice of an electronic payment system in drug clinical trials [J]. Chinese Journal of New Drugs, 2022, 31(08):784-787.
[3] Wu Lin, Yan Ting, Chen Yongfa. How to Construct a Provider Payment System Based on DRG——Enlightenment from the Practice of Japan, South Korea and Thailand [J]. Chinese Journal of Pharmaceuticals, 2022, 53(01):148-154.
[4] Gao Hong, Ning Hao. The Impact of the Merger and Restructuring of Urban Commercial Banks on the Payment System [J]. China Finance, 2022(05):61-62.
[5] Luo Hui, Wu Dianhua, Liang Di. Design of Guangdong Intercity Railway Public Transportation Multi-payment Ticketing System [J]. Urban Mass Transit, 2021, 24(12):130-135.
[6] Yao Yan, Niu Minglei, Sun Fajun, et al. Design and Implementation of Agricultural Transfer Payment Project Management System Based on Micro-Service Architecture [J]. Scientia Agricultura Sinica, 2021, 54(15):3207-3218.