E-commerce Trade Consumption Payment Security and Privacy Based on Improved B2C Model

Linzhu Hu
(Corresponding author: Linzhu Hu)

Chongqing University of Science and Technology
Campus city, Shapingba district, Chongqing 401331, China
(Email: lzhu1981@yeah.net)

(Received Sept. 22, 2018; revised and accepted Apr. 11, 2019; First Online May 26, 2019)

Abstract

With the popularity of the Internet and smart phones, e-commerce based on the Internet has rapidly developed by relying on its particular merits. However, the openness of the Internet makes payment security and privacy protection become the key of e-commerce development. This study gave a brief introduction of both traditional and improved Business to Customer (B2C) e-commerce and preformed the analogue simulation on shift left long (SLL) security protocol based on double encryption algorithm and traditional encryption algorithm under different sizes of data. The result showed that the double encryption algorithm could has lower complexity for encrypting and decrypting data, enabling to shorten the time of the encryption and decryption of the data; in terms of security, the decryption integrity of the data that was encrypted by double encryption algorithm was lower, and was basically garbled without logic. Thus, the security is guaranteed. In conclusion, the third-party privacy server in the improved B2C model can effectively guarantee the payment and privacy security of consumers.

Keywords: Business To Customer; Double Encryption Algorithm; E-Commerce; Payment Security

1 Introduction

With the popularity of the Internet, e-commerce, which is different from traditional commerce, has gradually developed. With the help of the Internet, e-commerce can initiate business transactions anytime and anywhere, and no physical cash is needed in this process [1]. However, for business operation, whether traditional or electronic, the most important thing is the protection of information [2], including transaction fund and personal information of both buyers and sellers [5,15].

Traditional business [18,21] is based on the real world, and in a state of "face to face", the buyer and the seller can completely rely on the only biological characteristic to confirm the information's reality and safety, but buyers and sellers of the electronic commerce with the virtual Internet cannot meet directly, so security protocol is used to ensure information security certification [6]. Studies on the e-commerce security are as follows. Yi *et al.* [14] brought up a formal analysis method to verify quantum cryptography electronic payment protocol security. The results showed that the agreement was not satisfactory because of the logical flaws. After improving and using formal analysis to verify again, it could be found out that defects were made up for. Mandal [16] put forward a kind of electronic payment system based on authentication key exchange protocol.

This case introduced an effective owner tracking mechanism to identify the malicious customers. At the same time, the automatic validation of the Internet security protocols and applications simulated the security of the scheme to prove that its replay and man-in-the-middle attack were safe. Mlke *et al.* [8] suggested to use a kind of privacy protection e-commerce protocol (PPEP) which would decouple or unlock online trade and consumer identity to provide anonymity for online shoppers in the e-commerce websites. What's more, they also brought up a PPEP plan which enabled merchants to perform customer management without disclosing the identity of customers to merchants. This study briefly introduced the traditional Business to Customer (B2C) and the improved B2C e-commerce model and simulated shift left long (SLL) security protocol based on double encryption algorithm and traditional encryption algorithm under different sizes of data.

2 Traditional B2C Model E-Commerce

As shown in Figure 1, the fundamental frame structure of traditional B2C mode [4,20] consisted of the third-party payment platform, buyer browser, seller website and logistics platform [12]. The execution flow of traditional B2C mode transaction protocol [7, 11] is shown by the ordinal arrow in Figure 1.

1) The buyer looks through goods in the seller website through the browser;
2) The seller provide goods information for buyers in the websites;
3) After logging in the website, buyer places an order for the goods and chooses the third-party payment platform to pay;
4) After receiving the payment order, the seller submits it to the third party platform;
5) The buyer confirms the payment transfer operation of the order in the third-party platform;
6) The third-party platform feed back the payment processing results to both the seller and the buyer;
7) The seller issues and processes orders and submits processing information to the third-party platform;
8) The buyer confirms the receipt of goods on the third party platform after he has received the goods satisfactorily;
9) The third-party platform transfers the buyer's payment to the seller's account.

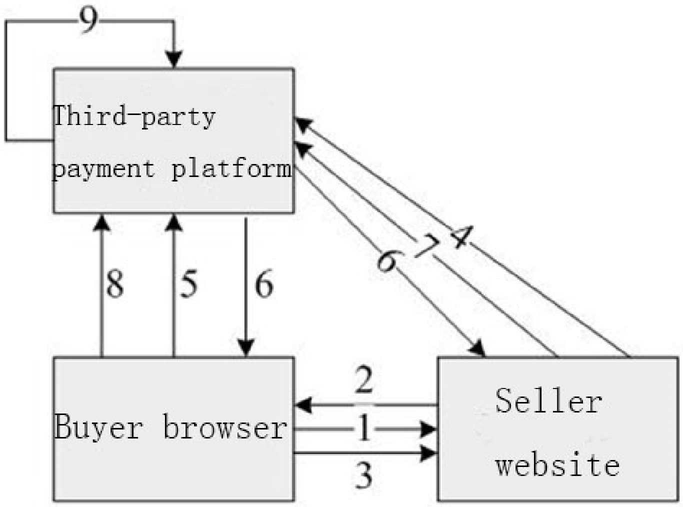

Figure 1: The traditional B2C mode model

Traditional B2C model adopts the third-party payment platform to ensuring the payment security, however, it still has some disadvantages in the physical application [3, 17]:

1) The seller is eager to deliver the goods after receiving the order without confirming the payment information of the buyer;
2) After the seller issues the goods, the buyer cancels the order due to malice or unexpected factors, resulting in the seller's property and goods being empty;
3) Because of the logistics platform, the seller delivers the goods, but the buyer who is "received" has not actually received the goods;
4) The order information of the buyer can be found on all three platforms in the circulation process, increasing the risk of privacy disclosure.

3 Improved B2C Mode E-Commerce

As shown in Figure 2, to solve the four shortcomings of the traditional mode mentioned above, the traditional B2C trade mode was expanded by third-party privacy server [9] and logistics platform, and the original functions of modules remain unchanged.

The execution flow of improved B2C mode transaction protocol is shown by the ordinal arrow in Figure 2 [13]:

1) The buyer browses the goods on the seller's website through the browser;
2) The seller provides the buyer with the commodity information on the website;
3) The buyer registers the address and other privacy information in the third-party privacy server, and obtains the corresponding ID serial number;
4) The third-party privacy server transfers the order to the seller;
5) The seller transfers the received order information to the third-party payment platform, where the privacy information in the order is replaced by the ID serial number obtained before;
6) Payment platform transfers the results of feedback to buyer and seller;
7) The seller delivers goods according to the order;
8) The logistics platform informs the buyer that the goods are received;
9) The logistics platform notifies the buyer's received information to the third-party privacy server;
10) Attending logistics platform can't learn the buyer's private information.

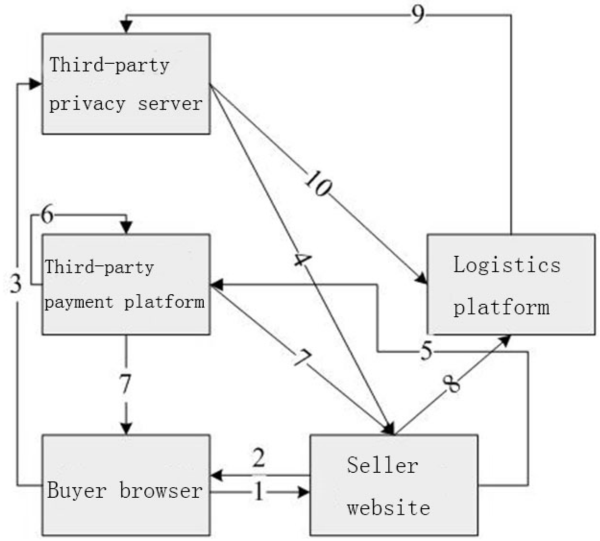

Figure 2: The improved B2C mode model

4 Double Encryption Algorithm

In the traditional B2C e-commerce model, the data interaction between modules is through Hyper Text Transfer Protocol (HTTP), but the data transferred by HTTP protocol transmission in general is the plaintext which has no encryption process. When conducting e-commerce transactions, data transferred is extremely easy to be intercepted or faked by a third party, meanwhile, the both sides of transmitting and receiving information can't confirm identity of each other. In the improved B2C e-commerce model, third-party privacy server and logistics platform are added. The third-party privacy server provides the whole model with Secure Socket Layer (SSL) security agent protocol based on double encryption algorithm [22]. SSL protocol can provide secure communication privacy protection for both sides of data transmission.

As shown in Figure 3, the third-party privacy server will judge the data type after receiving it from the buyer's browser, and if it is PI, the flag bit of SSL will be flag1=0, flag2=0; then the public key of the payment gateway in the SSL protocol is used to encrypt the PI, and obtain the payment encryption package CPI, which is then filled into the actual data recorded in the SSL protocol. If it is an order information OI, it is populated directly into the actual data in the SSL record; after obtaining the actual data recorded by SSL, the Hash function algorithm is applied to perform summary calculation on the actual data, the sequence generated by the sequence generator and the encryption key of PI. The obtained summary data was MAC data. The SSL record generated in the first few steps shall be encrypted by applying the symmetric key [10,19] in the SSL protocol negotiated by both parties to generate the transmission ciphertext Crecord-SSL.

The double encryption algorithm mentioned above is

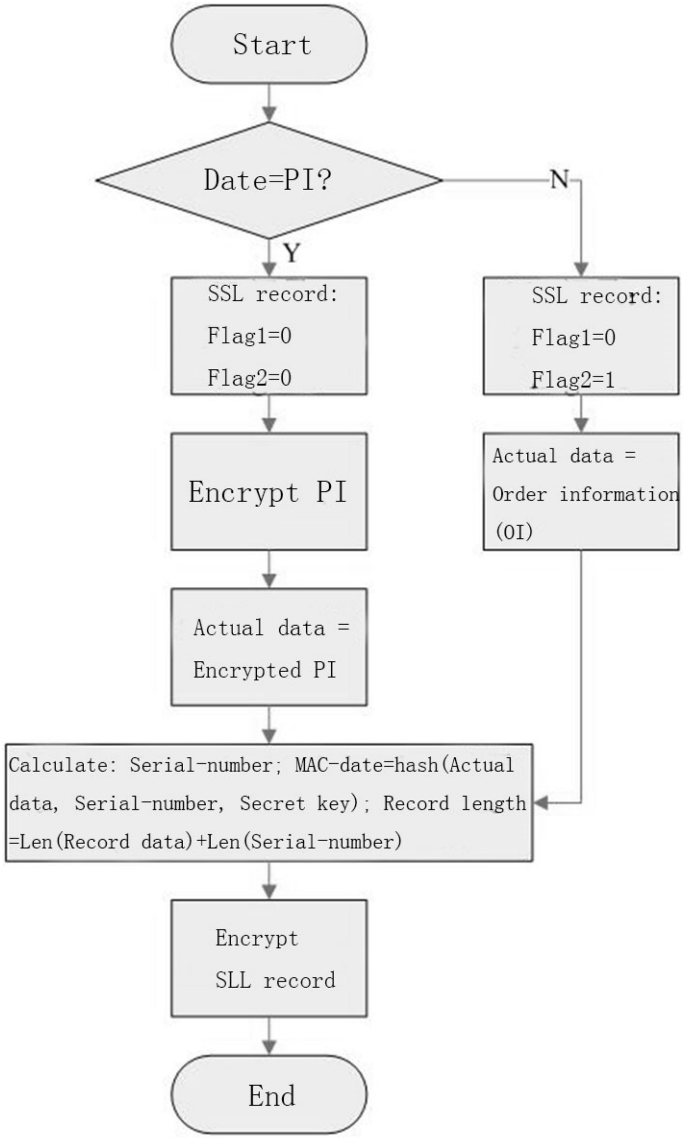

Figure 3: Double encryption algorithm flow

applied in the third-party privacy server to obtain the ciphertext Crecord-SSL of payment information and order information, and then transmitted to the server of the seller's website. After receiving ciphertext Crecord-SSL, the server performs symmetric decryption according to the negotiated symmetric key, then checks the integrity of SSL record data, and judges whether the record data is order information or payment information according to the flag bit. If it is the order information, the server will extract the information and put it into storage for processing. In the case of payment information, the payment encryption package CPI will be transmitted to the third-party payment platform, and the public key of the payment gateway is used to decrypt it and wait for the payment result. If successful, the logistics platform is informed to deliver the goods.

5 Simulation Experiment

5.1 Experiment Environment

The experiments in this study were performed on a lab server with server configuration of Windows 7 system, I7 processor, and 16 Gbytes of memory. The coding of SSL security protocol based on double encryption algorithm and SSL security protocol based on double encryption algorithm was implemented using C++.

5.2 Experiment Methods

Data packets with different sizes of order information and payment information were set, and data packets were encrypted and decrypted through SSL security protocol based on double encryption algorithm and SSL security protocol based on double encryption algorithm. The experiment was repeated 100 times and the average of the total time required to encrypt and decrypt the data packets under both algorithms was counted.

Similarly, data packets with different sizes of order information and payment information were set, and the data packets were encrypted respectively through SSL security protocol based on double encryption algorithm and SSL security protocol based on double encryption algorithm. Then the encrypted data packets were informally decrypted to simulate the situation where the orders and payment information were stolen, meanwhile, the maximum decryption time was set as 60 min to prevent the decryption time from being too long. The cracked ciphertext was compared with the original text to obtain the decryption integrity.

5.3 Experiment Results

5.4 Time Complexity

As shown in Figure 4, for a data packet of 1 M, the total time required for encryption and decryption by the traditional encryption algorithm was 78.7 ms, and the total time of the double encryption algorithm was 31.2 ms; for a data packet of 10 M, the traditional encryption algorithm required 600.3 ms, and double encryption algorithm required 245.1 ms; for a data packet of 20 M, the traditional encryption algorithm needed 1181.5 ms, the double encryption algorithm needed 487.2 ms; for a data packet of 30 M, the traditional encryption algorithm needed 1765.9 ms, the double encryption algorithm needed 695.3 ms; for a data packet of 40 M, the traditional encryption algorithm required 2377.5 ms, and the double encryption algorithm required 1103.2 ms. It could be seen that no matter which algorithm was, as the data to be encrypted increased, the total time required for encryption and decryption increased, and the difference of the required time between the two algorithms became increasingly obvious starting from 10 M, and the time required by the double encryption algorithm was significantly smaller than that of the traditional algorithm. It showed that the double encryption algorithm had lower time complexity and better performance.

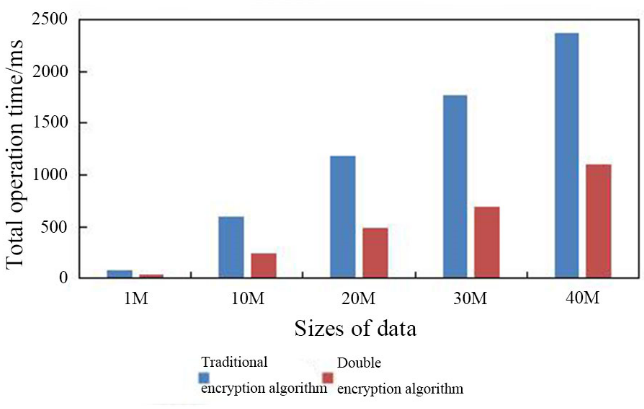

Figure 4: Total time of encryption and decryption of different sizes of data by different algorithms

5.5 Security Analysis

As shown in Figure 5, after 60 minutes of decryption, the integrity of the traditional encrypted data packet of 1 M was 10.2%, and the integrity of the double encrypted data packet was 8.1%; the integrity of the traditional encrypted data packet of 10 M was 8.2%, and the integrity of the double-encrypted data packet was 5.3%; the integrity of the traditional encrypted data packet of 20 M was 5.1%, and the integrity of the double-encrypted data packet was 3.2%; the integrity of the traditional encrypted data packet of 30 M was 2.2%, and the integrity of the double-encrypted data packet was 0.8%; the integrity of the traditional encrypted data packet of 40 M was 0.9%, and the integrity of the double encrypted data packet was 0.2%. It could be seen that with the increasing of the encrypted data packet, the integrity of the decrypted data was significantly reduced. After the data packet of 1 M was decrypted for 60 minutes, it could be seen that there were several logical characters. In the situation of the data packet of 20 M, only a few logic characters were available. In the situation of the data packet of 40 M, the decrypted data was basically garbled. Both algorithms could prevent decrypting to a certain extent, and the decrypted data which was encrypted by double encryption algorithm had lower complexity and higher safety.

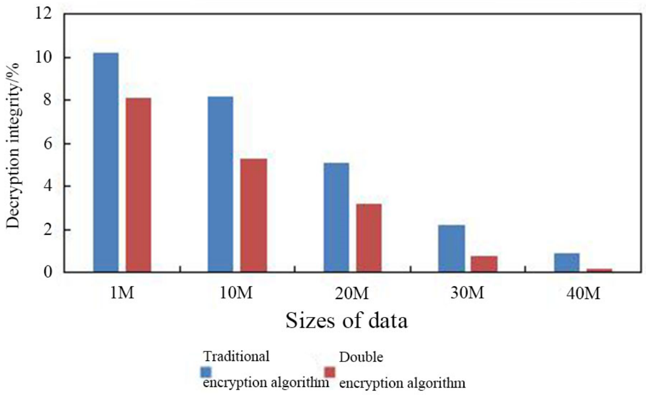

Figure 5: Security of encryption of different sizes of data by two algorithms

6 Conclusion

This article simply introduced the traditional B2C and improved B2C of e-commerce model. The improved electronic business model of B2C compared with the traditional one increased two modules as a third party privacy and logistics platform. Third party privacy server used SSL security protocol based on double encryption algorithm to improve the payment security and privacy protection of e-commerce. Then, the performance of SLL security protocol based on double encryption algorithm and traditional encryption algorithm in encrypting data of different sizes was simulated. The result was that the total time required for encryption and decryption of both algorithms increased with the increase of encrypted data.

The double encryption algorithm had less time complexity and less total time for decryption and encryption, and was more suitable for private information exchange of e-commerce. It was found that the data packet with larger size had significantly reduced decryption complexity after 60 min decryption of the data packet encrypted by the two encryption algorithms. Both algorithms could prevent decrypting to some extent, and the data that was encrypted by the double encryption algorithm had lower decryption integrity and higher security. To sum up, the added third-party privacy server based on double encryption algorithm in the improved B2C e-commerce mode can ensure the security of payment and privacy.

References

[1] S. A. Chaudhry, M. S. Farash, H. Naqvi, *et al.*, “A secure and efficient authenticated encryption for electronic payment systems using elliptic curve cryptography,” *Electronic Commerce Research*, vol. 16, no. 1, pp. 113–139, 2016.

[2] Z. Djuric, D. Gasevic, “FEIPS: A secure fair-exchange payment system for internet transactions,” *The Computer Journal*, vol. 58, no. 10, pp. 2537–2556, 2015.

[3] T. H. Feng, M. S. Hwang, and L. W. Syu, “An authentication protocol for lightweight NFC mobile sensors payment,” *Informatica*, vol. 27, no. 4, pp. 723–732, 2016.

[4] E. Y. Huang, C. J. Tsui, “Assessing customer retention in B2C electronic commerce: an empirical study,” *Journal of Marketing Analytics*, vol. 4, no. 4, pp. 172–185, 2016.

[5] M. S. Hwang, C. C. Lee, Yan-Chi Lai, “Traceability on low-computation partially blind signatures for electronic cash”, *IEICE Fundamentals on Electronics, Communications and Computer Sciences*, vol. E85-A, no. 5, pp. 1181–1182, May 2002.

[6] M. S. Hwang, Li-Hua Li, “A New Remote User Authentication Scheme Using Smart Cards”, *IEEE Transactions on Consumer Electronics*, vol. 46, no. 1, pp. 28–30, Feb. 2000.

[7] M. S. Hwang, I. C. Lin, L. H. Li, “A simple micropayment scheme”, *Journal of Systems and Software*, vol. 55, no. 3, pp. 221–229, Jan. 2001.

[8] M. Ike, K. Sarac, “PPEP: A deployable privacy preserving e-commerce protocol for electronic goods,” in *International Conference on Communication & Network Security*, 2016.

[9] S. E. Kaplan, R. J. Nieschwietz, “A web assurance services model of trust for B2C e-commerce,” *International Journal of Accounting Information Systems*, vol. 4, no. 2, pp. 95–114, 2015.

[10] M. M. Kiani, A. Raza, K. D. Gill, “Centralized collaborative reputation model for B2C E-Commerce,” *17th IEEE International Multi Topic Conference*, pp. 450–455, 2014.

[11] N. Knego, “Importance of assortment for B2c electronic commerce in some EU countries,” *Economy & Business Journal*, vol. 10, no. 1, pp. 94–102, 2016.

[12] I. C. Lin, M. S. Hwang, C. C. Chang, “The general pay-word: A micro-payment scheme based on n-dimension one-way hash chain”, *Designs, Codes and Cryptography*, vol. 36, no. 1, pp. 53–67, July 2005.

[13] J. Ling, M. Jun, Z. Yang, “Customer-perceived value and loyalty: how do key service quality dimensions matter in the context of B2C e-commerce?,” *Service Business*, vol. 10, no. 2, pp. 301–317, 2016.

[14] Y. Liu, X. Liu, J. Wang, *et al.*, “Security analysis of electronic payment protocols based on quantum cryptography,” in *International Conference on Information Science & Control Engineering*, IEEE, 2017.

[15] J. W. Lo, H. M. Lu, T. H. Sun, and M. S.Hwang, "Improved on date attachable electronic cash," *Applied Mechanics and Materials*, vol. 284, pp. 3444–3448, 2013.

[16] S. Mandal, S. Mohanty, B. Majhi, "Design of electronic payment system based on authenticated key exchange," *Electronic Commerce Research*, vol. 18, no. 2, pp. 359–388, 2018.

[17] D. L. Paris, M. Bahari, N. A. Iahad, "Business-to-customer (B2C) electronic commerce: An implementation process view," in *3rd International Conference on Computer & Information Sciences*, pp. 19–24, 2016.

[18] M. Pasquet, S. Gerbaix, "Instant payment versus smartphone payment: The big fight?," in *IEEE Third International Conference On Mobile And Secure Services (MobiSecServ'17)*, pp. 1–3, 2017.

[19] L. G. Pee, "Customer co-creation in B2C e-commerce: does it lead to better new products?," *Electronic Commerce Research*, vol. 16, no. 2, pp. 1–27, 2016.

[20] M. S. Hwang and P. C. Sung, "A study of micro-payment based on one-way hash chain", *International Journal of Network Security*, vol. 2, no. 2, pp. 81–90, Mar. 2006.

[21] S. Walczak, G. L. Borkan, "Personality type effects on perceptions of online credit card payment," *Journal of Theoretical and Applied Electronic Commerce Research*, vol. 11, no. 1, pp. 5, 2016.

[22] X. Wang, Y. Jia, L. Guo, "Study on the function of computer technology in the electronic commerce environment security and risk assessment," in *International Conference on Intelligent Transportation*, pp. 784–786, 2016.

Biography

Linzhu Hu, born in 1981, gained the master's degree from China University of Petroleum. She is working as a lecturer in Chongqing University of Science & Technology. Her research direction is international business and trade. She had hosted and participated in the project: In 2013, she participated in the school-level education reform project "Research on the Construction of Applied Talents Training Platform for International Economics and Trade Majors Based on Discipline Competition"; In 2015, she participated in the school-level teaching reform project "Application Research of CLIL Bilingual Teaching Model Based on Applied Undergraduate Brand Characteristics"; In 2016, she guides students to participate in the first prize of the Cross-Strait College Students International Trade Competition; In 2017, she hosted the school-level "Business Negotiation Practice" "School Plan" project.