Research on e-commerce payment security and privacy protection based on improved B2C model

Zhihe Wang

Received: August 3, 2020. Revised: August 28, 2020. Accepted: September 1, 2020. Published: September 2, 2020.

Abstract**—**The popularity of Internet and mobile terminals promotes the development of e-commerce. However, e-commerce which is not necessary to face to face poses a major challenge to the payment security and privacy protection of consumers. This paper briefly introduces the traditional business to customer (B2C) e-commerce model. A third-party privacy server was introduced to provide a double encryption algorithm for the model, and then the traditional and improved B2C models were simulated to verify the performance of the two models in the confidentiality of the transaction information and the security of the transaction information transmission process. The results showed that the intruder could not directly obtain the sensitive privacy information such as payment information and order information of consumers even if he invaded the database of the online store when the improved B2C model was used; after the transaction information was intercepted and decrypted under the two B2C models, the decryption integrity decreased with the increase of the transaction information quantity, while under the same transaction information quantity, the decryption integrity of the improved B2C model was lower.

Keywords**—**Business to customer, e-commerce, encryption algorithm, payment security.

I. Introduction

WITH the popularization of Internet and mobile terminals, some offline business activities are gradually transferred to online, i.e., e-commerce is gradually emerging [1]. Different from the traditional offline business activities, the emerging e-commerce is based on the Internet, and most transactions, except for special requirements, do not need cash. Whether it is online or offline business operation, it is crucial to protect the information security of both sides of transaction [2]. In particular, online e-commerce does not need face-to-face communication like offline commerce, so both sides of the transaction can not confirm the true identity of the other party, increasing the risk of information disclosure. The existence of security protocol has become a guarantee for the security of information authentication of both parties of transaction [3]. Yi et al. [4] applied the formal analysis method to verify the security of the electronic payment protocol of quantum cryptography and found that the protocol was not satisfactory due to the logic defects. After improvement, the formal analysis was used again to verify the protocol, and they found that the defects were well made up. Mandal et al. [5] proposed an electronic payment system based on the authentication key exchange protocol. In this scheme, an effective owner tracking mechanism was introduced to identify malicious customers. Moreover, the security of the scheme was simulated in the automatic verification of Internet security protocol and application tools, which verified that the scheme was safe against replay and man-in-the-middle attacks. Ike et al. [6] proposed a privacy protection e-commerce protocol (PPEP) which decoupled or unlocked the online transaction and the customer's identity to provide anonymity for online shoppers in the e-commerce website and also proposed a PPEP scheme to enable businesses to implement customer management without disclosing the customers' identity to businesses. This paper briefly introduces the traditional business to customer (B2C) e-commerce model. Then a third-party privacy server was introduced to provide a double encryption algorithm for the model, and the traditional and improved B2C models were simulated to test the performance of the two models in the confidentiality of the transaction information and the security of the transaction information transmission process. In this study, a third-party privacy server was added to the original traditional B2C model to enhance the security in the process of B2C transactions. Then, the simulation experiments were carried out on the traditional and improved B2C models. The final results showed that the improved B2C model was more excellent in transaction information encryption, and the improved B2C could maintain a stable verification when facing the increasing amount of transaction information. The contribution of this paper is to provide an effective reference for e-commerce transaction information encryption.

II. Traditional B2C E-commerce Model

As shown in Fig.1, the basic structural framework of the traditional B2C mode [7] includes the third-party payment platform, buyer's browser, seller website, and logistics platform. The buyer's browser is the abstract representation of customer. The seller website is the abstract representation of merchant or enterprise. The third-party payment platform is the payment system, and it realizes the transfer operation between the buyer and seller by associating the bank accounts of customers who register in the platform with the third-party accounts that register in the platform after signing a contract with banks. Moreover, as the third-party payment platform has the independent domain name, it can ensure the security of transactions when the customer pays. The common third-party

Z. H. Wang is with the School of Business, Hunan University of Humanities, Science and Technology, Loudi, Hunan 417000, China (e-mail: hwk3080@163.com).

payment platforms include Alipay, Tenpay, banks [17], etc. Fig. 1 also includes the use process of the traditional B2C model. Firstly, the customer applies for opening their own accounts in the payment platform (this step only appears in the first use of a third-party payment platform); secondly, the customer uses the Internet to browse the goods or service information provided by the online store, places orders on demand, and provides the online store with their own account information in the payment platform; thirdly, the online store initiates a transfer application to the payment platform with the account information provided by the customer [8]; fourthly, the payment platform verified the transfer application and transferred after verification; fifthly, the payment platform feeds back the transfer processing result of the order to the online store; finally, the online store notifies the customer after receiving the feedback result of the payment platform and contacts the logistics company for distribution of commodity [9].

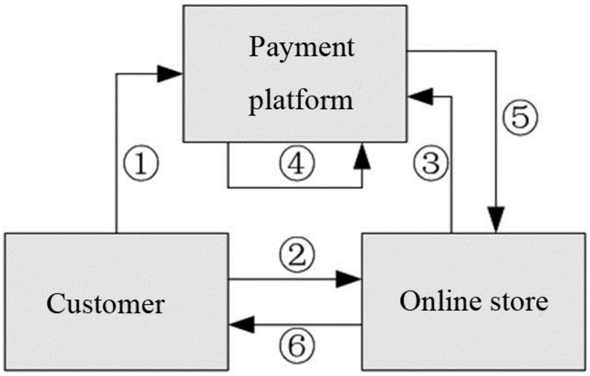


Fig. 1 The traditional B2C e-commerce model

Although the traditional B2C mode uses the third-party payment platform to ensure the security of payment, there are the following shortcomings in the practical application [10]: (1) the seller is eager to deliver the goods after receiving the order and may fail to confirm the buyer's payment information; (2) after the seller sends out the goods, the buyer may cancel the order due to malicious or unexpected factors, resulting in the seller’s loss of money and goods; (3) the seller delivers the goods, the logistics platform shows that the buyer has received the goods, but the buyer does not actually receive the goods; (4) the buyer's order information can be found in the three platforms in the circulation process, which increases the risk of privacy disclosure.

III. Improved B2C E-commerce Model

As shown in Fig. 2, compared with the traditional model, the improved B2C e-commerce model is added with the third-party privacy server [11], and the other three composition structures have no changes in function. The third-party privacy server added in the improved model can store and forward the sensitive information of business activities, i.e., the three objects participating in business activities in the traditional model do not interact with each other directly, but through the third-party server. In the process of storing and forwarding sensitive information, the third-party privacy server will use encryption algorithms to encrypt the data, and the two parties use the corresponding key when contacting with the third-party server, which further ensures the security of the information. The arrow with serial number in Fig. 2 is the execution process of the model, and the details are shown below.

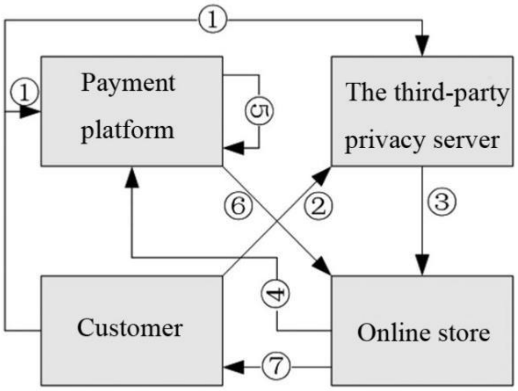


Fig. 2 The improved B2C e-commerce model

The flow of the improved B2C model in Fig. 2 is as follows. Firstly, the customer opens the corresponding account in the payment platform and the third-party privacy server (generally only appears in the first use of a third-party payment platform and privacy server). Secondly, the customer uses the Internet to browse the goods or service information provided by the online store, and places an order according to the demand, and the order which contains sensitive information such as account, password, address and contact information is transmitted to the third party privacy server. Thirdly, the third party privacy server encrypts the sensitive privacy information of the order to generate relevant address ID label and transmits it to the online store. Fourthly, after the online store receives the order, the store verified the ID label in the order on the third party server and transmitted the order information to the payment platform. Fifthly, the client logs in the payment platform, and the payment platform completes transfer according to the order information. Sixthly, the payment platform notifies the online store with the payment result, the online store contacts the logistics company to deliver the good and uploads the order information which contained the address ID label to the third party server to gain a temporary two-dimensional code, and the logistic company can only obtain relevant information through the two-dimensional code. Finally, the online store feeds back the processing result to the client, the payment platform will transfer the payment to the online store after the user confirms the receipt of the good, and moreover the third party server will invalidate the temporary two-dimensional code.

As mentioned above, the third-party privacy server is added in the composition structure of the improved B2C model to encrypt the transaction information in the transmission and storage. The payment platform, customers, and online stores will not have direct information exchange with each other, but indirectly through the third-party server. The information they can obtain from the third-party server is only the information allowed by their authority, and they can not query the information beyond the authority. The existence of the third-party server greatly improves the confidentiality of information, but the third-party server has limited resources generally. If the third-party server is directly invaded, the security performance will greatly reduce. The blockchain technology that emerges in recent years is a kind of distributed ledger database, and its characteristics, such as decentralization, consensus algorithm, hash encryption, etc., makes it competent for the privacy encryption requirement of the third-party server. The decentralization of the blockchain makes the data transmitted by the three parties be stored in blocks of the blockchain distributively. Once someone tampers with a block, the other blocks can identify and correct it by the consensus algorithm.

In addition to the application of B2C model in e-commerce, B2C model can also be applied in stock exchange [16]. In this process, both sides of securities trading are similar to customers and online stores in e-commerce, and the stock exchange can be regarded as the payment platform. In order to ensure the security of transactions, the information is encrypted and stored by the third-party server.

IV. Secure Socket Layer (SSL) Protocol

Whether it is traditional B2C model or improved B2C model, SSL protocol will be used in data transmission. SSL protocol has been widely used in identity authentication and data security transmission in the Internet. SSL protocol can effectively prevent the information between different Internet users from being eavesdropped and tampered. Its content consists of handshake protocol and record protocol. The handshake protocol is used to ensure the establishment of a secure connection between two users, and the record protocol is used to ensure the security mode of data transmission. In the process of using handshake protocol, client and server will negotiate data encryption algorithm, encryption and decryption key and mutual authentication. When the handshake protocol successfully establishes a secure connection between the client and server, the record protocol will use the negotiated encryption algorithm to encapsulate the transmission data. The record protocol includes record header and record data. The record header is divided into two types: two bytes and three bytes, which simply summarizes the type and length of the data to be transmitted. The record data includes MAC, actual data and filling data in the aspect of form. MAC can check the integrity of the data. The actual data are the data to be transmitted. The filling data is the data after encrypting the actual data with block algorithm. In terms of security, SSL protocol can effectively prevent interception and man-in-the-middle attacks. The reason is that the encryption algorithm negotiated by both parties will be used when using the protocol for communication, and the key generated temporarily will be used for each connection. Even if the key is in plaintext during the interaction, the RSA exchange key has good key protection ability due to its own mathematical characteristics.

V. Encryption Algorithm

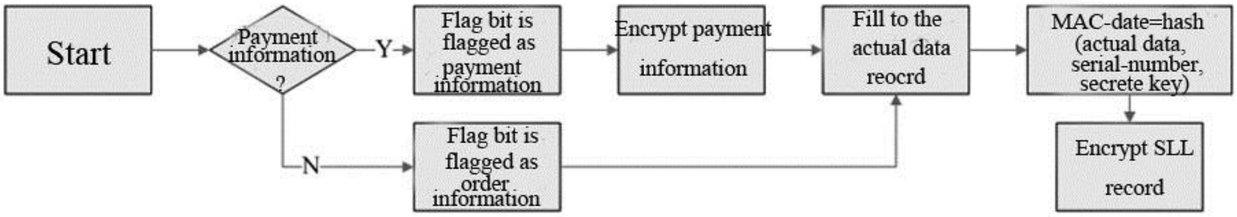

Start
Payment information ?
Y
N
Flag bit is flagged as payment information
Encrypt payment information
Fill to the actual data reocrd
MAC-date=hash (actual data, serial-number, secrete key)
Flag bit is flagged as order information
Encrypt SLL record

Fig. 3 The flow of the encryption algorithm

In the e-commerce transaction process, the interaction information among customers, payment platform and online store is usually payment information and order information, which are equal in importance. However, payment information often contains important information such as the bank account password of customers. Compared with order information, once payment information is leaked, the loss will be greater. Therefore, double encryption will be made for payment information [12], and its overall flow is shown in Fig. 3.

① Firstly, the third-party server will judge whether the data type is payment information or order information after receiving the information from the customer.

② If it is judged as payment information, flag1=0 and flag2=0 are flagged at the flag bit of SSL record, and the next step is to encrypt the payment information: the payment encryption package CPI is obtained using the public key of payment gateway in SSL protocol.

③ If it is judged as order information, flag1=0 and flag2=1 are flagged at the flag bit of SSL record.

④ The order information or encrypted payment information are filled into the actual data of SSL record, then Hash function algorithm is applied to make summary calculation on the actual data, sequence generated by sequence generator and the key of the encrypted PI, and the summary data obtained are MAC data.

⑤ Finally, the SSL records generated in the previous steps are encrypted with the symmetric key [13] in the SSL protocol negotiated by both parties to generate the transmission ciphertext Crecord-SSL.

After obtaining the ciphertext Crecord-SSL of payment information and order information by the above double encryption algorithm in the third party privacy server, it is transmitted to the server of the seller website. After the server receives ciphertext Crecord-SSL, it is processed by symmetric decryption according to the negotiated symmetric key, and then the integrity of the SSL record data is checked. Whether the record data are order information or payment information is judged according to the flag bit. If the data are order information, the server will extract the information and store it; if the data are payment information, it transmits the payment encryption package CPI to the third party for payment platform for decryption of the public key [14] with payment gateway. If the payment is successful, the logistics platform is notified to deliver the good.

VI. Simulation Experiment

A. Experimental environment

The experiment was carried out on a laboratory server. The server configuration was Windows 7 system, i7 processor and 16 G memory. SSL security protocol based on double encryption algorithm was realized by C + + [15], and components of B2C model were simulated by different servers.

B. Experimental Setup

In this study, four servers were set up to simulate the client, online store, payment platform and third-party privacy server. The four servers were all in the LAN of the laboratory, and the communication was smooth and unimpeded. Then the following experiments were carried out.

(1) Test on the confidentiality of B2C model for payment information and order information before and after improvement

The order information and payment information were randomly input into the client, for example, “order no. 1001, mobile phone, one, customer name abc, customer address no. XX, XX road” and “merchant no. 1001, client credit card no. 333564, payment amount 1200.00, payment password 123567”. Then the transaction information was transfered according to the process of the traditional B2C and improved B2C models respectively. In this process, invasion to the database of the online store was simulated. As this experiment was to verify the confidentiality of the two models, rather than the anti-invasion ability of the database, the login password was directly given to simulate the success of the invasion, and the transaction information in the database was queried.

(2) Test on the transaction information transmission security of B2C model before and after improvement

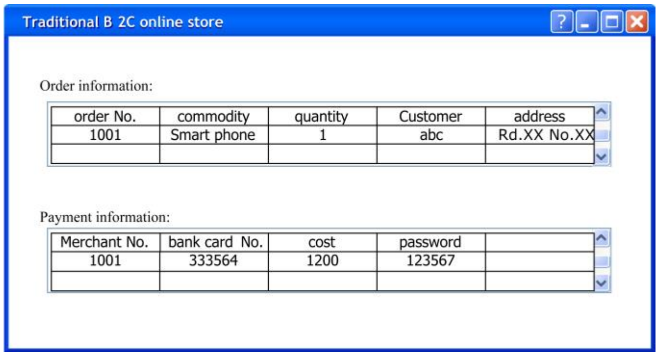
As before, the order information and payment information were input randomly into the client, and then the transaction information was transferred according to the process of the traditional B2C and improved B2C model respectively. In this process, the transaction data transmitted to the online store was intercepted and cracked to obtain the corresponding transaction information. In the above process, different amount of transaction information was set, and the maximum interception and cracking time was set as 60 min to prevent the cracking time from being too long. The cracked ciphertext was compared with the original text to get the integrity of the decryption.

(3) Test on the stability of the improved B2C model

The improved B2C model is applied to business activities, and its stability needs to be guaranteed in the use process. Therefore, it is necessary to test its stability. The stability test was mainly about the stability of the model system under multiple transaction information. Firstly, many transaction information were randomly generated according to the form of the first two experiments, and then the stability test was conducted on groups of 10, 20, 30, 40, 50, 60, and 70 transaction information. Moreover, transaction information whose amount was the same with the above groups was input into the model system, and the transmission success rate was recorded. The traditional model also performed the same operation as a control group.

C. Experimental Results

The database intrusion of online store under the two B2C models was simulated. In order to facilitate the experiment, the login password was directly given to simulate the situation after the successful intrusion, and the database intrusion results of online store under the two B2C models are shown in Fig. 4 and 5. Fig. 4 is the intrusion result of online store database under the traditional B2C model. The order information and payment information of customers were intuitively seen, and the important privacy information such as bank card number and payment password in payment information could be directly obtained. Fig. 5 is the result of the online store database intrusion under the improved B2C model. Compared with the traditional model, the order information that could be directly queried after the intrusion under the improved model only included the order number, commodity name, quantity and customer name, the payment information could only find the merchant number and payment amount, the address in the order information and the bank card number, payment password and other important privacy information in the payment information were all converted into underlined asterisks which were links. The asterisks were connected with the third-party server, and specific information could only be obtained after inputting corresponding password. In order words, under the improved B2C model, neither the merchant nor the intruder could get the complete transaction information directly from the database, especially the sensitive privacy information, which greatly improved the confidentiality.



Traditional B 2C online store

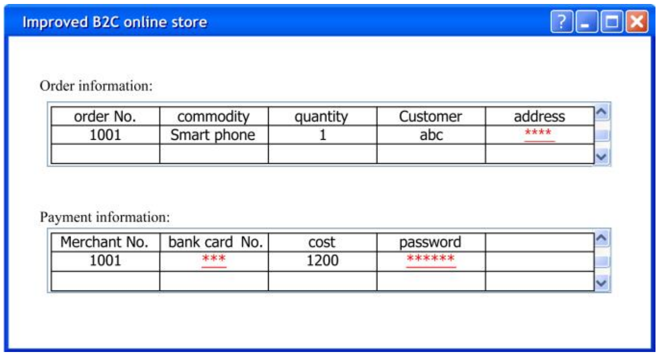
Order information:

order No.	commodity	quantity	Customer	address
1001	Smart phone	1	abc	Rd.XX No.XX

Payment information:

Merchant No.	bank card No.	cost	password	
1001	333564	1200	123567	

Fig. 4 The intrusion results of the traditional B2C online store



Improved B2C online store

Order information:

order No.	commodity	quantity	Customer	address
1001	Smart phone	1	abc	****

Payment information:

Merchant No.	bank card No.	cost	password	
1001	***	1200	******	

Fig. 5 The intrusion results of the improved B2C online store

The traditional B2C model guaranteed the fairness and security of the transaction to a certain extent due to the intervention of the third-party payment platform, and it encrypted the data during the data transmission to ensure the security of the transmission to a certain extent. However, under the traditional B2C model, the encryption of data transmission was only a conventional single encryption. Under the improved B2C model, a third-party privacy server was introduced, and a double encryption algorithm was provided in the third-party privacy server. The security of transaction information transmission of the two models is shown in Fig. 6. It was seen from Fig. 6 that the decryption integrity of the two models gradually decreased with the increase of the number of transaction information to be processed after 60 minutes of interception and decryption, and moreover the decryption integrity of the improved B2C transaction information was lower under the same number of transaction information. It showed that the transaction information transmitted by the two models was both protected, and the improved B2C model was more strict in the protection of transaction information transmitted.

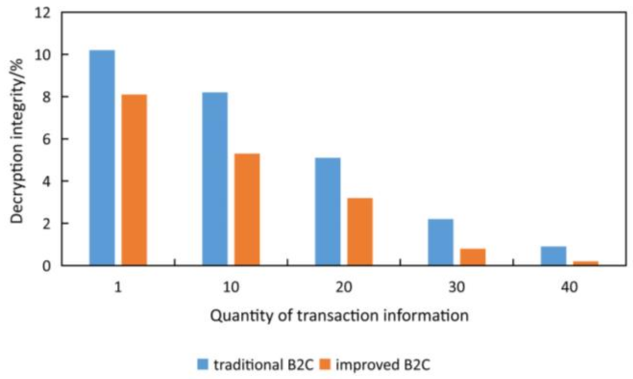


Fig. 6 The security of transaction information transmission by the model before and after improvement

The application of B2C model often faces with large-scale trading activities; therefore, ensuring its stability is an important factor affecting the service quality of e-commerce. The delivery success rate of the improved B2C model is shown in Fig. 7. It was seen from Fig. 7 that the success rate of the traditional B2C model decreased gradually with the increase of the transaction information transferred in the model, while the success rate of the improved B2C model was always maintained at 100%. The information transmission, storage, and encryption in the traditional B2C model were carried out on their own platforms, and the resources of individual platforms were limited. Once the information needed to be processed increased, the computing resources would be short, leading to the failure of information transmission. In the improved B2C model, due to the addition of the third-party server, it shouldered the transmission, storage, and encryption of information, the three parties involved in transaction activities browsed and downloaded information in the server through their own key, which greatly reduces the computing load. Therefore, as long as the third-party server has enough computing resources, it can process the transaction information stably.

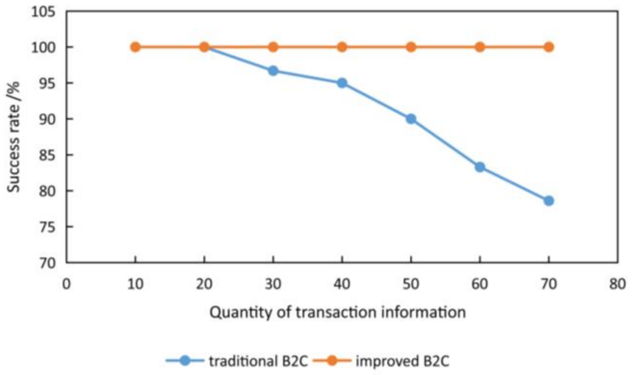


Fig. 7 The success rate of multiple transaction information before and after improvement of the B2C model

VII. Conclusion

This paper briefly introduced the traditional B2C e-commerce model and introduced the third-party privacy server as an improvement. The third-party privacy server provided a double encryption algorithm for the model, and then the B2C model before and after the improvement was simulated to verify the confidentiality of the transaction information and the security of the transaction information in the transmission process. The results are: (1) under the traditional B2C model, the complete transaction information including bank card number, payment password and customer address was easily queried after intruding into the online store database; under the improved B2C model, only the basic information was queried after invasion, and the client related sensitive privacy information could only be queried through the authentication of the third party privacy server; (2) with the increase of the number of transaction information, the decryption integrity of the transaction information under the two models both reduced; when the number of transactions was the same, the decryption integrity of the intercepted transaction information was lower under the improved B2C model.

REFERENCES

[1] S. A. Chaudhry, M. S. Farash, H. Naqvi., and M. Sher, "A secure and efficient authenticated encryption for electronic payment systems using elliptic curve cryptography," *Electron. Commer. Res.*, vol. 16, no. 1, pp. 113-139, Jun. 2016.

[2] Z. Djuric, and D. Gasevic, "FEIPS: A Secure Fair-Exchange Payment System for Internet Transactions," *Comput. J.*, vol. 58, no. 10, pp. 2537, Oct. 2015.

[3] S. Walczak, and G. L. Borkan, "Personality Type Effects on Perceptions of Online Credit Card Payment," *J. Theor. Appl. El. Comm.*, vol. 11, no. 1, pp. 5-5, Jan. 2016.

[4] Y. Liu, X. T. Liu, J. Wang, L. Zhang, and C. J. Tang, "Security Analysis of Electronic Payment Protocols Based on Quantum Cryptography," in *International Conference on Information Science & Control Engineering*, Changsha, China, 2017.

[5] S. Mandal, S. Mohanty, and B. Majhi, "Design of electronic payment system based on authenticated key exchange," *Electron. Commer. Res.*, no. 6, pp. 1-30, Nov. 2016.

[6] M. Ike, and K. Sarac, "PPEP: A Deployable Privacy Preserving E-Commerce Protocol for Electronic Goods," in *International Conference on Communication & Network Security*, 2016.

[7] M. Pasquet, and S. Gerbaix, "Instant payment versus smartphone payment: The big fight?" in *2017 Third International Conference On Mobile And Secure Services*, 2017.

[8] E. Y. Huang, and C. J. Tsui, "Assessing customer retention in B2C electronic commerce: an empirical study," *J. Market. Anal.*, vol. 4, no. 4, pp. 172-185, Jan. 2017.

[9] N. Knego, "Importance of assortment for B2c electronic commerce in some EU countries," *Econ. Busin. J.*, vol. 10, pp. 10, 2016.

[10] D. L. Paris, M. Bahari, and N. A. Iahad, "Business-to-customer (B2C) Electronic Commerce: An implementation process view," in *International Conference on Computer & Information Sciences*, 2016.

[11] S. E. Kaplan, and R. J. Nieschwietz, "A Web assurance services model of trust for B2C e-commerce," *Int. J. Account. Inform. Syst.*, vol. 4, no. 2, pp. 95-114, Jun. 2003.

[12] J. Ling, M. Jun, and Z. Yang, "Customer-perceived value and loyalty: how do key service quality dimensions matter in the context of B2C e-commerce?" *Serv. Busin.*, vol. 10, no. 2, pp. 301-317, Feb. 2015.

[13] X. Wang, Y. Jia, and L. Guo, "Study on the Function of Computer Technology in the Electronic Commerce Environment Security and Risk Assessment," in *International Conference on Intelligent Transportation*, IEEE, Halong Bay, Vietnam, 2015.

[14] L. G. Pee, "Customer co-creation in B2C e-commerce: does it lead to better new products?" *Electron. Commer. Res.*, vol. 16, no. 2, pp. 1-27, Apr. 2016.

[15] M. M. Kiani, A. Raza, and K. D. Gill, "Centralized collaborative reputation model for B2C E-Commerce," in *Multi-topic Conference*, Karachi, Pakistan, 2014.

[16] A. Ribaj, O. Ilollari, F. Scalera, "The unethical banking costs distrust of bank customers (Albania case as a model for SEE countries)," *WSEAS Trans. Busin. Econ.*, vol. 16, pp. 582-592, 2019

[17] A. Zemάnkovά, "Artificial intelligence and blockchain in audit and accounting: literature review," *WSEAS Trans. Busin. Econ.*, pp. 568-581, Volume 16, 2019

Zhihe Wang, born in 1972, has received the master's degree. He is an associate professor in Hunan University of Humanities, Science and Technology. He is interested in e-commerce.