Research on Smart City Smart City E-commerce Security Technology Based on SET Protocol

Gengyi Xiao
Department of Mathematics and Computer Technology, Guilin Normal College, Guilin, China
gengyixiao@glnc.edu.cn

Abstract. Secure Electronic Transaction (SET) has always been regarded as an international security standard followed by smart city e-commerce. It generally uses public key cryptography and digital certificates and other related technologies, which can help solve a series of security problems in the development of smart city e-commerce. The above security issues are designed to include the confidentiality of shopping and payment information, the completeness of transactions, the exactness of identity and non-cheating. The completeness and integrity of information are guaranteed in the link of electronic transactions. However, this agreement has its shortcomings in that it is costly and operational review. Based on this background, the paper reviews the application of SET protocol in e-commerce, and hopes to provide relevant suggestions for its development and improvement.

Keywords: Smart city e-commerce, encryption, decryption, authentication centre, SET protocol.

1. Introduction
With the popularization and development of the Internet, traditional business activities have also changed from the traditional face-to-face transaction model to the electronic transaction model. The emergence of smart city e-commerce has greatly facilitated transactions between commercial enterprises, between commercial enterprises and consumers, and between consumers and consumers. While providing consumers with convenient and fast services, it also enhances the competitiveness of enterprises, which greatly promoted economic development and social progress [1]. Electronic online payment has become the main component of smart city e-commerce and has been favoured by all parties. However, the security of smart city e-commerce, that is, the confidentiality of information, the correctness of information, the integrity of information, and the indispensability of transactions Denial has become a bottleneck restricting its development. How to realize the security and confidentiality of online transactions is a problem that must be solved. Various security protocols have been gradually developed, among which SET protocol has gradually become a security protocol standard, but there are also certain defects in the transaction process.
2. SET protocol and its security technology

The Secure Electronic Transaction SET protocol was developed by Visa and MasterCard (the two famous credit card organizations in the world), and it is a payment specification designed for online transactions of bank credit card payments.

2.1. The main features of the SET protocol

The application of SET protocol is designed to encrypt the message information related to bank credit card payment transactions to ensure that the information is safely transmitted on the Internet network and the transmitted data will not be intercepted or stolen [2]. But it cannot encrypt arbitrary data (such as text or images) like the SSL protocol; the working process of the SET protocol involves three parties, namely customers, merchants, and banks, and these three parties have digital verification and mutual authentication to determine communication the identity of the other party; order information and personal bank credit card account information are separated from each other. When sending an order including cardholder account information to the merchant, the merchant can only see the order information, but not the cardholder's account information. This is the most critical feature in the SET protocol, and its realization is the application of dual digital signature technology.

2.2. The working principle of the SET protocol

In a SET payment transaction, three software's are mainly used, namely, browser wallet, merchant server, and payment gateway. In SET transactions, there are mainly three parties involved, namely, customers (also cardholders), merchants, and commercial banks (including card issuing banks and merchant banks). Customers, also known as cardholders, in the smart city e-commerce environment, customers use computers to communicate with merchants through the Internet, purchase goods and services they are satisfied with, and then use bank cards issued by the issuing bank (such as debit cards, credit cards) etc. for settlement. In the conversation between the customer and the merchant, the SET protocol ensures that the cardholder's account information will not be leaked. When merchants provide goods or services, they use the SET protocol to ensure the safety of personal information. The merchant who accepts card payments must have a relationship with the bank [3]. Commercial banks include the card issuing bank and the merchant's account opening bank. The card issuing bank issues a bank card for each customer who establishes account information and guarantees the payment of each certified transaction; the merchant's account opening bank is the online transaction merchant opening settlement the bank of the account. Sometimes, the card-issuing bank and the merchant’s bank may be the same bank.

The following example illustrates the working principle of the SET protocol by taking a customer using the Internet smart city e-commerce purchase company's online product process as an example. First, the customer uses the browser to view the online product catalogue and browse the products on the merchant’s Web homepage; Second, the customer selects the product to be purchased, fills in the order, including the item list, price, total price and other cost information; third, the customer chooses the payment method and tells the merchant that the bank credit card will be used for payment. At this time, the SET agreement begins to intervene; fourth, the merchant sends the item list and a unique transaction identifier to the customer, and also sends its merchant certificate, including the merchant’s disclosure the key is sent to the customer, as well as the bank's certificate, including the bank's public key. These two certificates are encrypted with the secret key of the same certification centre CA; Fifth, the customer uses the certification centre CA public key to decrypt the two certificates, and obtains the public key of the merchant and the public key of the merchant's account bank. The customer generates and sends two data packets: complete order information and payment instruction information. The order information packet includes the transaction identifier and the type of credit card used, but does not include account information such as credit card numbers. The payment instruction packet includes the transaction identifier, the customer's credit card account number and password, and the agreed payment amount. The order information data is encrypted using the merchant’s public key, and the payment instruction data is encrypted using the public key of the merchant’s account opening bank. Sixth, the
merchant receives two data packets, processes the order information data packets, and generates a message at the same time [4]. The text includes the authorization request for the credit card payment request generated by the merchant (the authorization request includes the transaction identifier), the payment instruction packet sent from the customer, and the merchant's certificate, and the message is encrypted and sent to the merchant with the public key of the merchant's account bank. Seventh, the merchant bank receives this message, decrypts it, and checks whether it has been tampered with, and whether the transaction identifier in the authorization request is consistent with the customer's payment instruction packet. After checking that the message is legal, the merchant's account bank sends a message requesting payment authorization through the settlement communication channel between banks. Once the customer's card issuing bank approves the payment, the merchant's account bank sends an encrypted response message including the transaction identifier to the merchant; eighth, after the merchant receives its account bank's response information, it also sends the customer a response message of successful online purchase. This message serves as a receipt and informs the customer: "The payment has been accepted, and the purchased items will be sent out soon." So far, the process of an online transaction of smart city e-commerce activities is over. The SET protocol works from the third step to the end. Figure 1 shows the SET model.

2.3. Double signature technology

Dual signature technology is an important innovation of digital signature technology in SET protocol. Among them, the consumer sends the order information OI to the store separately, and at the same time sends the payment instruction PI to the bank. In this way, the consumer's payment information and consumption information are separated, that is, the store does not know the consumer's bank card number and other content, and the bank does not know the consumer’s order and shopping details, effectively protecting the consumer’s privacy. However, under necessary circumstances, these two kinds of information can be linked together to resolve certain disputes or doubts and further ensure the interests of consumers. Dual signature technology realizes the "isolated and connected" state of consumer related information. The main principle is shown in Figure 2 on the following page:
3. Analysis of SET protocol security issues in smart city e-commerce transactions

3.1. The security of the current SET protocol in smart city e-commerce transactions

3.1.1. Identity authentication. This is mainly achieved through dual signatures. Since the transaction process of smart city e-commerce is carried out online, the two parties in the transaction cannot communicate face-to-face. However, through dual signatures, the consumption information and payment instructions of the relevant personnel can be authenticated by the relevant identity, thereby enabling the merchant or bank to perform subsequent operations [5]. In other words, the merchant will only arrange the delivery after confirming the consumer information about the consumer, and the bank will only make the corresponding payment after confirming the legal identity of the cardholder to achieve identity authentication.

3.1.2. Information confidentiality. Mainly through information encryption, that is, through the combination of public key encryption (RSA) and private key encryption (DES). Among them, the relevant information is processed according to the DES data encryption standard, and then further encrypted by RSA, which is equivalent to sealing the relevant encrypted data. Therefore, the combination of these two technologies forms a "digital envelope", which makes the information the transmission process has higher confidentiality. At present, due to the rapid development of computing and technology, both RSA and DES algorithms have certain security threats. However, it can often be controlled by lengthening the key length. For example, the current secure RSA key length should be at least Greater than 1024bit.

3.1.3. Information integrity. Under the SET security protocol, the Hash function is often processed through the information summary during the data transmission process, so that the relevant data will generate the corresponding Hash value, and the value is unique and one-way, that is, There is a strict correspondence between the data bits in the message and the information summary, and it is almost impossible for different messages to produce the same information summary, and at the same time, it is impossible to reversely obtain the relevant message question through the information summary. Finally, the message is transmitted together with the information summary, ensuring the integrity of the information.

3.1.4. Irresistibility. Under the framework of the SET protocol, when both parties to the transaction send information, they need to be digitally signed. The digital signature is realized by the transaction’s own private key. This private key is usually only the user’s own customs declaration. Therefore, once the
information is sent, whether it is the sender Neither the receiver nor the receiver can deny its own participation in the message, thus ensuring the non-repudiation of the message.

3.2. Security issues of current SET protocol in smart city e-commerce transactions

First of all, in the encryption and decryption process of SET, often only RSA algorithm and DES algorithm can be used, which makes its adaptability and flexibility greatly compromised. At the same time, due to the continuous improvement of current computer computing speed, its encryption algorithm is cracked the possibility of this has also increased greatly, posing a huge threat to the information security of customers. Secondly, the SET protocol does not clarify issues such as the retention of evidence in the transaction process [6]. Once a problem occurs, not only there is no corresponding arbitration institution, and the evidence cannot be effectively used, as shown in Figures 3 and 4.

![RSA Algorithm Flow Chart](image)

**Figure 3.** RSA algorithm flow chart

![DES Algorithm Flow Chart](image)

**Figure 4.** DES algorithm flow chart
4. Analysis of the corresponding countermeasures for the security issues of the SET protocol in the smart city e-commerce transaction process

4.1. Selection of Encryption Scheme

4.1.1. Overlay encryption scheme. The nested encryption scheme is also known as the nested encryption scheme. Its main implementation process is divided into three steps: firstly, the relevant message is encrypted independently; secondly, the SET default method is adopted to encrypt the message and send it; again, the receiver first Use the SET default method for decryption, and then perform autonomous decryption. Although this scheme takes a little longer than the original scheme, it not only has higher security, but also breaks through the limitation of the SET protocol in encryption and decryption algorithms, and thus has higher adaptability. In addition, the scheme has Flexible scalability, repeated nesting can be carried out, which further expands the application range of the SET protocol.

4.1.2. Negotiate encryption schemes. This scheme draws on the method of the SSL protocol, that is, before the information exchange, the two parties of the transaction determine the encryption and decryption algorithms of the data through a certain handshake agreement, so that they can reach a consensus, that is, the two parties organize their own encryption algorithms to generate the algorithm identifier list. And exchange and match, so as to confirm the algorithm that both parties can use, and encrypt relevant information [7]. This algorithm is slightly lower in efficiency, but its security is relatively higher. At the same time, it also breaks through the algorithm limitations of the SET protocol and improves its adaptability.

4.2. Countermeasures for security issues in different periods of transaction

4.2.1. Early trading period. In the early stage of the transaction, issues such as privacy protection and "non-refusal behaviour" should be resolved. Before a transaction is concluded, allowing customers to make self-selection is enough to open their own information, digitally sign the selection results, and then formulate relevant binding contracts, and keep a copy in both parties and the CA centre, and the CA centre will treat the credit, Supervise, record and announce the breach of contract. At the same time, for "non-refusal behaviours," merchants and customers can agree on different digital certificate verification methods, and then clarify and restrict the rights and rules of both parties.

4.2.2. After the transaction. Mainly resolve disputes about the quality of goods or services. For such problems, the traditional "deposit" rules can be resolved. On the one hand, the disputes between the parties to the transaction can be resolved more simply. On the other hand, it is conducive to the formation of a tacit understanding between the parties in the transaction process and enhance mutual trust. In this way, not only can the interests of consumers be protected, but also merchants can be encouraged to improve the quality of their products and services, and thus the quality disputes between the two parties can be avoided to the greatest extent.

5. Conclusion
In the process of e-commerce in smart cities, the security of transaction information is the most concerned issue, and the SET protocol provides certain specifications for it, which has high practical value. Therefore, we should speed up the resolution of the existing problems. To make the SET protocol more perfect and serve the vigorous development of smart city e-commerce.

Acknowledgments
This work was financially supported by Guangxi university scientific research fund: Research on the key technologies of vehicle-mounted network based on CPS (2013YB286).
References

[1] Khorsheed, K. O. A Comparative Study between (AES) and (DES) Algorithms Based on the (SET) Protocol. Kirkuk university journal for scientific studies, 13(3) (2018) 64-74.

[2] Lee, W. H., Miou, C. S., Kuan, Y. F., Hsieh, T. L., & Chou, C. M. (2018). A peer-to-peer transaction authentication platform for mobile commerce with semi-offline architecture. Electronic Commerce Research, 18(2), 413-431.

[3] Das, S. K., Yadav, A. K., & Tripathi, S. IE2M: Design of intellectual energy efficient multicast routing protocol for ad-hoc network. Peer-to-Peer Networking and Applications, 10(3) (2017) 670-687.

[4] Ogundoyin, S. O. A privacy-preserving certificateless two-party authenticated key exchange protocol without bilinear pairing for mobile-commerce applications. Journal of Cyber Security Technology, 3(3) (2019) 137-162.

[5] Gunasinghe, H., & Bertino, E. PrivBioMTAuth: Privacy preserving biometrics-based and user centric protocol for user authentication from mobile phones. IEEE Transactions on Information Forensics and Security, 13(4) (2017) 1042-1057.

[6] Ehikioya, S. A., & Zhang, C. Real-time multi-agents architecture for E-commerce servers. International Journal of Networked and Distributed Computing, 6(2) (2018) 88-98.

[7] Vij, S. R., Mukhopadhyay, D., & Agrawal, A. J. Automated Negotiation in E Commerce: Protocol Relevance and Improvement Techniques. CMC-COMPUTERS MATERIALS & CONTINUA, 61(3) (2019) 1009-1024.