A safe trading model based on encryption hybrid algorithms for mobile electronic commerce

Hong Li[1a],Guoyou Shi[2b]

[1]Professional Department,Beijing Information Technology Collegeline ,Beijing，China

[2]Technology Office,Beijing Municipal Bureau of Archives,Beijing，China

[a]yalian0627@126.com, [b]yangguang0627@126.com

Keywords-Mobile electronic-commerce; Encryption hybrid algorithms, Transaction risk ; Security specifications

Abstract. With the rapid development of mobile communication technology, mobile electronic-commerce as a new type of electronic-commerce is attracting widespread attention and use because of his advantages, such as simple, usable, fast, convenient and suitable cost. but how to ensure fast and convenient transactions, raising transaction security and reduce transaction risk is the main problem faced by mobile electronic-commerce, to solve this problem, a safe trading model based on Encryption hybrid algorithms for mobile electronic commerce was proposed, which has all security specifications to beneficial for all related persons in mobile Electronic commerce.

Introduction

With the rapid development of information technology, the financial industry has highly become e-enabled. Updates of the technology and network construction are accelerated. Advanced trading tools such as mobile electronic commerce, have been rapidly promoted and applied in the financial industry. Current network security, trade disputes and other issues is the main problem faced by mobile e-commerce, how to ensure fast and convenient transactions, raising transaction security and reduce transaction risk is the urgent research projects to solve.

Problems of existing mobile e-commerce payment models

Currently, there are four mobile e-commerce payment models in Mobile commerce market: operators - centric model, bank-centric model, point to point mode model, cooperation model and there are two main aspects to distinguish between different types of electronic payment model:

A. Relationship

Who dominant the relationship (fund payments, bill payments, account, etc.) between ultimate users, banks, carriers and other non-banking companies;

B. Rules

There are different rules hidden between the natural and banks and non-bank companies and institutions.

These three models has both advantages and disadvantages, the following mainly describes their problems:

C. The problems of operator-centric model

In the operator-centric model, mobile phone operators act independently for the performance of electronic payment and financial institutions, but do not participate in the payment process. In this mode, the operator is the production manager authority and electronic payments.

Many developed operator-centric models have been challenged as a result of no relationship with current payment networks. Some examples have been entrusted with such electronic payment methods and models in emerging countries, but they do not cover the electronic payment services, and they have been limited to the purchase of fund payments and mobile phone charging. Payment

with credit card and payment through telecommunication phone bill. Here, you can pay in two ways. Thus, in this model, major expenditure is not supported.

There are two major problems, one problem is how to introduce a set of products and services for payment and how to introduce the solution which can be accepted as a safe and reliable method, and the other problem is the acceptance of this model , Because there are issues, such as privacy and imitation, lack of commercial relations between merchants and operators, centralization of POS equipment to the seller, and Mistrust of billing and service provided by the operators, so that merchants and consumers accept this model at the same time is very difficult.

D. The problems of bank-centric model

Bank-centric model also has two problems. Firstly, because of excessive dependence to the mobile phone operators, all banks may be forced to support the operator's different and special standards, and secondly, banks trade bill to invest in the production of electronic payment account of their non-contact debit and credit cards.

E. The problems of point to point mode model

This model is different from the above model. The third company provides electronic payment services as an independent financial institutions and network operators. It uses banks and operators of infrastructure, build a bridge contact for customers, vendors and banks.

Due to over-reliance on third company, lack of product quality and financial supervision, it is prone to trade disputes arising caused by product quality issues, and money laundering caused by unfunded regulatory ,as well as the financial security issues caused due to network security.

F. The problems of Cooperation model

Cooperation model include trust cooperative banks, operators and third-party companies. Service Manager is responsible for all payments and collaborative process management operators and banks. This model allows beneficiaries to focus on their primary function, and gradually open the door to earn new revenue service, direct retention and customer loyalty, and meet the needs of major customers. Therefore, it is more difficult to implement and build collaborative model. Despite relations between actors of this model, their cooperation is very complex.

Safe Trading Model based on Encryption hybrid algorithms for mobile E- commerce

In order to solve the problems of the above model, a safe trading model based on encryption hybrid algorithms was proposed, it includes six elements: Customers, Merchant, Trusted third company(TTC), Electronic trading platform software, Costumer's bank and Merchant 's bank.

G. Organization elements

- Consumers purchase goods via mobile devices trading platform;
- Merchant sells electronic goods and provide some services;
- Electronic trading platform is the software installed on the consumer's mobile devices, jointly certified by consumers, merchants and banks. Consumers contact the merchant and the bank through the software, and then complete the mobile Electronic commerce, the software uses encryption protocol to encrypt messages and delivered to the mobile user subscription for using the mobile communication service;
- Trusted third company plays two important roles: issue secure digital certificates for bank and as settlement payments between banks;
- Costumer's bank is responsible for managing the consumer's bank account, authenticate consumers, and conducted cash flow between consumers accounts, communications and Merchant 's bank;
- Merchant’s bank is responsible for managing the Merchant’s bank account. It is the consumer banking and credit the seller's bank account registered TTC using digital certificates for cash flow and exchange. As showed in figure 1.

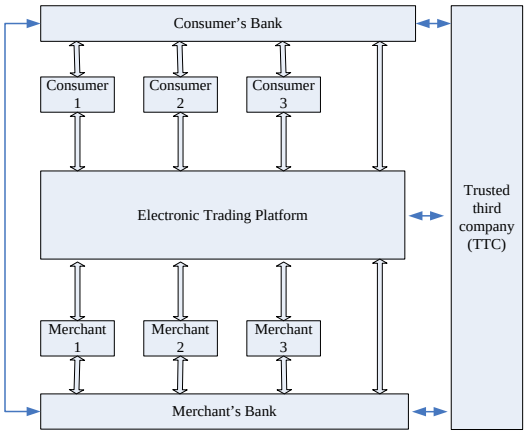

Fig1.Organization Chart of the proposed model

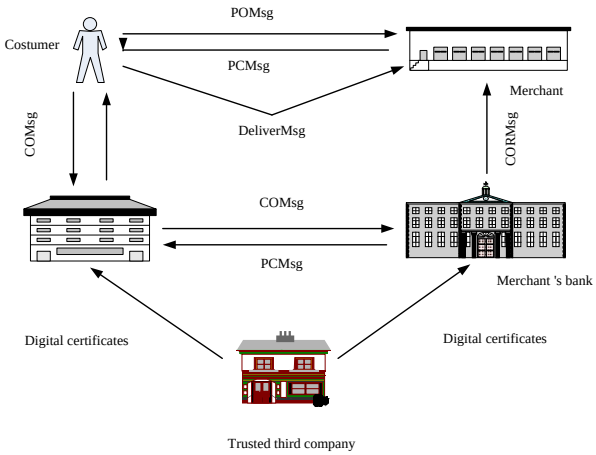

Fig2. Main elements and transaction process

H. Transaction process

As illustrated in figure 2, Transaction process consists of the following links:

- Firstly, consumers view merchant's website to select the desired goods purchased. Electronic Trading Platform generates the "Product Orders message (POMsg)", which contains the consumer's name, address, ID number, and the number and categories of goods, and then sends it to the merchant.
- Secondly, when the merchant receives the "POMsg" message from consumers, Electronic Trading Platform generates purchase bills for consumers and encrypts it using the public key, and sends it to the consumer. This message includes some details of the price, currency, and selected product description. Consumers check the product description and price, in order to ensure the accuracy of selection.
- Thirdly, consumer receives message from the merchant, decrypt and generate "Confirm Order message (COMsg)", use this message from his bank and pay for the goods.

- Fourthly, consumer's bank receives "COMsg" message, then use the private key verification and inspection costumer account whether there is sufficient amount of load consumption or not. Since then, it debits accounts as required by costumer price, and generates "Confirm Order responding message (CORMsg)". This message is signed by the costumer bank's private key. In addition, it uses the merchant's bank public key encryption to avoid manipulation. Encrypted messages sent to the merchant's bank, while the confirmation message is sent back to the consumer.
- Fifthly, when the merchant's bank receives the message, decrypts and verifies it, and checks the costumer's bank signatures and time accuracy expiration information. Subsequently, the merchant's account is a credit and "Payment confirmation message (PCMsg)" is sent to the consumer and the consumer's bank.
- Sixthly, when consumer's bank has received the "PCMsg" message from the merchant's bank, immediately sends a verification message to the consumer.
- Finally, when the merchant has received the "CORMsg" message from his own bank, immediately provides demand products to consumer.

Features of the proposed model in ensuring transaction security and efficiency

The model has five measures to ensure the security of transaction. They are data integrity, non-repudiation, authentication, confidentiality and hybrid encryption. Data integrity guarantee the content of the message cannot be operated and changed.

I. Data integrity:

It ensures that the content of the message can not be operated and changed, and the message is unchanged.

The sender generates a message and uses his own private key to encryption the message. The client separates summary of message and decrypts it using the sender's public key. If these digests match, the sender is claiming one of data integrity are met.

J. Non-Repudiation:

This characteristic prevents fake claim of a person who has not performed any transactions Signatures provide nonrepudiation of performed operations.

Non-repudiation can prevent a person who has not carried out any false claims transaction signatures provide accreditation to perform the operation, the seller and the consumer co-sign the receipt, in order to avoid refusal transaction by the merchant or consumer.

K. Authentication:

Message authentication refers to prove the consistency of the original identity of the receiver. Verify the identity of the person who is the same person who claims.

In this protocol, authentication via digital signatures secure encryption mechanism. The sender should sign the message with their private messages. The client checks the accuracy of the signature using the sender's public key. If the signature is valid the sender is authenticated.

L. Confidentiality:

It prevents unauthorized people from accessing sensitive payment. This information could lead to abuse of the future.

When the merchant receives "POMsg" message from the consumer, sends the bill and the shared key to the consumer. The consumer receives the message, decrypts it, and generates "COMsg" messages and pay for the products.

Consideration of efficiency and safety

M. Efficiency

- Symmetric encryption is performed very quickly in a mobile device with high efficiency, for there only one key is used for encryption and decryption, Thus, efficiency of the system will be ensured. AES method is used in he messages which only the public key had been used, and suitable for micropayment.
- Asymmetric encryption and digital signatures are time consuming and may affect the efficiency of the mobile device system, but it's more secure than symmetric method, and it uses to encrypt and decrypt both public and private keys.

Because ECC method can calculate the digital signature and decrypt the data at very high speeds, and its security is higher than that of other asymmetric algorithms. Therefore, we choose ECC asymmetric encryption among asymmetric encryptions to improve efficiency and speed of encryption calculation.

N. safety

Asymmetric encryption and digital signatures are not suitable for the use of micro-payments, but it is completely in line with the logic of micro-payment because it requires high security.

Based on the above considerations, the proposed model is a hybrid encryption method, which uses AES algorithm to encrypt small transactions, other transactions using the ECC asymmetric encryption, because digital signature is calculated and data is decrypted with very high speed in ECC method and its security is higher than that of other asymmetric algorithms

Conclusion

On the basis of analysis the Problems in existing mobile e-commerce payment models, a safe

trading model based on Encryption hybrid algorithms for mobile electronic commerce was proposed, which use data integrity, non-repudiation, authentication, confidentiality and hybrid encryption methods to ensure security and efficiency of the transaction, because beneficiaries have almost equal risk and benefit, it is better than other models.

References

[1] HAN X.M, "The application of web technology in electronic commerce", 2009 International Conference on Computer Technology and Development(ICCTD 2009), IEEE Press,.2009: pp.636-640.

[2] LIN C, PENG X.H. "Research on network architecture with trustworthiness and controllability",Journal of Computer Science and Technology,Volume 21- No. 5, May 2006,pp. 732-739.

[3] RAO Y, FENG B.Q, "Web service-oriented dynamic E-Business integration framework", Computer Integrated Manufacturing Systems, Volume 10- No. 11, November 2004,pp. 1454-1458.

[4] Omkar Ghag, Saket Hegde, " A Comprehensive Study of Google Wallet as an NFC Application", international Journal of Computer Applications,Volume 58- No. 16, November 2012,pp.1123-1131.

[5] AJese, B. K, Philemon E. D, Falaki, S. O, "Comparative Analysis of Public-Key Encryption Schemes",.International Journal of Engineering and Technology, Volume 2- No. 9, September 2012,pp. 329-337.

[6] Sung-Woon Lee, Hyun-Sung Kim, Kee-Young Yoo, “ A Passwordbased Efficient Key Exchange Protocol”, KIISE Journal, Vol. 31 No.04, 2004, pp.347-352.

[7] Men Long, Uri Blumenthal, "Manageable One-Time Password for Consumer Applications", IEEE International Conference on Consumer Electronics (ICCE 2007), IEEE Press,2007, pp.10-14.

[8] Lance J. Hoffman, Kim Lawson and Jeremy Blum," Trust beyond security: An expanded trust model", Communications of the ACM vol. 49-No. 7, July 2006,pp. 95-101.