Exploratory Autopsy on Digital Payment Models

Tao Wang & Changsu Kim & Kisu Kim

Management Information System Division, School of Management, Yeongnam University, Korea
Dae-dong 214-1, Keongsan-si, Keongbuk 712-749, Korea

Abstract

Secure digital payment is critical in the successful shaping of global digital business. Digital payments are increasingly being used as a substitute to traditional payments, contributing markedly to the efficiency of the economy. The focus of every digital business transaction is to minimize risks arising from transactions. It is essential to ensure the security of digital payment whether used in internal networks or over wireless Internet.

This paper analyses secure digital payment methods from the viewpoint of systemic security and transaction security. According to comparative analysis of digital payment models, this paper proposes a comparative analysis framework to investigate and evaluate secure digital payment. In conclusion, the comparative analysis framework, comparison of digital payment models and mobile payment models proposes a useful academic and practical foundation to enhance the understanding of secure digital payment methods. It also provides academic background and practical guidelines for the development of secure digital payment systems.

Keywords: Digital Payment Model; Comparative Analysis Framework, Mobile Payment Model

I. Introduction

New digital technologies have been applied to change the way business is conducted (Laudon & Traver, 2001). This paper focuses on four types of digital payment models. These models have been frequently used in the past or anticipated to be the most popular in the near future. In this paper, an overview of these secure payment models is presented and an attempt is made to evaluate these models. After then, an attempt to provide a secure mobile digital payment model is achieved by analyzing the existing digital payment models.

This paper is organized as follows. First, we deal with the theoretical background of digital payment, focusing on an overview of digital payment, an overview of digital payment risk and previous research on secure digital payment. Second, on the basis of review on digital payment types and digital payment models, this research proposes a comparative analysis framework to analyze different types of digital payment models. Third, this research will carry out comparative analysis on four types of digital payment models and summarize them. Forth, a mobile digital payment model is proposed for the future of secure mobile digital payment. Finally, the paper ends with a summary of conclusions as well as suggestions further research issues.

II. Theoretical Background of Digital Payment

2.1 Overview of Digital Payment

Digital payment has several advantages compared to traditional payments; there are many modern digital payment methods in existence due to the diversity of payment usage in different situations. The methods of online digital payment can be divided into three categories: 1) Cash, transactions are settled with the exchange of digital currency. A well-known example of on-line currency exchange is digital cash (Hsieh, 2001; Laudon & Traver, 2001; Wright, 2002; Slyke & Belanger, 2003). 2) Credit cards, the server authenticates customers and communicates with the bank to verify that funds are sufficient before purchase (Korper & Ellis, 2000; Hsieh, 2001; Slyke & Belanger, 2003). Electronic checks, financial institutions pay a given amount to the payee electronically between the buyer and seller's bank. (Wright, 2002; Lawrence et al., 2002; Slyke & Belanger, 2003).

2.2 Overview of Digital Payment Risk

Security can generally be defined as a set of procedures, mechanisms and computer programs to authenticate the source of information and guarantee the integrity and privacy of the information to minimize the chance of situations that could lead to damage of data or network resources (Hai, 2005).

Many of the risk categories associated with emerging digital payment technologies can be divided into 1) service risk, 2) privacy risk 3) transaction risk (Laudon & Traver, 2001; Fajfar, 2004). A more detailed account of the digital payment risk is as follows.

2.2.1 Service Risk

One of the risks faced by users of online payment services is the possibility that a payment service will commit an inadvertent error and intentionally misappropriate funds or discontinue service (Lawrence & Newton, 2002).

2.2.2 Privacy Risk

This risk relates to the use and potential misuse of personal information by online payment services. Since these services are largely unregulated, online payment services are generally free of legal constraints on collection and use of personal data (Laudon & Traver, 2001). Since payment services may share personal data with one another and with other financial service providers, a payment service tends to cause personal information about the buyer to be revealed to the seller.

2.2.3 Transaction Risk

When transaction information is transferred on the Internet, many transaction risks exist (Mantel & McHugh, 2003). These risks include tampering with encrypted information, important financial information disclosure and fraud behavior. Typically, these risks always exist. Attention should be given to these risks and an effective secure method should be taken to ensure security during transactions (Hai, 2005).

2.3 Previous Research on Secure Digital Payment

To acquire useful insights of issues that could affect the security of digital payments, this section reviews previous research related to the security of digital payments. In focusing on security of digital payments, it is hoped to provide valuable insights and a foundation for tracing the issues relevant to the security of digital payments.

Kalakota and Whinston (1997) examined some of the issues associated with the security of digital payments. They mentioned that secure digital payments should be hardened against all forms of attack and the vulnerability of the system to attacks via the Internet should be considered. This study reveals that security attacks will take the form of passive eavesdropping, modification of messages, impersonation and attacks against the computer involved in the transaction.

Laudon and Traver (2001) investigated issues that have been identified as being important in secure digital payments. They believe that security success for digital payments is attributable to a number of factors: refutability, risk for consumer and merchant, anonymity for consumer and merchant, security against unauthorized use, authentication requirements and hardware requirements.

Pilioura (2001) provided an evaluation method for secure digital payment; two categories of factors were identified: security principles and privacy. This means that payment systems require adherence to some fundamental security and privacy principles that cryptography greatly enhances. These principles are authentication, integrity, double-spending prevention, payment confidentiality, payment anonymity and payer untraceability.

Slyke and Belanger (2003) examined existing digital payment security technologies such as encryption (SSL and SET protocol) and authentication (digital signature and digital certificates). They concluded that secure digital payment should provide security against fraudulent activity.

Romdhane (2005) investigated the security evaluation approach for digital payment systems. This study argued that secure digital payment 1) should consist of the following requirements: integrity, authentication, fraud prevention and privacy; and 2) should have these properties: divisibility, transferability, double-spending prevention, confidentiality, anonymity and payer untraceability.

Table 1. Summary of previous research on Digital Payment

Researcher	Domain	Issues
Kalakota and Whinston (1997)	Issues associated with digital payment security	Passive eavesdropping Active modification of messages Impersonation Attacks against the computer
Laudon and Traver (2001)	Important factors of digital payment security	Refutable (able to be repudiated) Financial risk Anonymous Security against unauthorized use Tamper-resistant Authentication Special hardware required
Pilioura (2001)	Evaluation approach of secure digital payment	Authentication Payment integrity Double-spending prevention Loss-tolerance Nonrepudiation Confidentiality, anonymity Payer untraceability
Slyke and Belanger (2003)	Digital payment security technology	Encryption (SSL & SET) Authentication (digital signature and digital certificates)
Romdhane (2005)	Security evaluation approach for digital payment system	Integrity Authentication Fraud prevention Privacy

Based on the above review of previous research on secure digital payment systems, it is reasonable to classify the variables that have been identified into two groups: systems and transaction security. During the transaction process, consumers are sensitive to risks against personal privacy and information integrity. According to the review, authentication and the ability to issue refunds are also necessary transaction security issues for a secure digital payment model. Systems security is the basis of digital transactions. In this paper, new systems security research variables, such as a special network and special institution are added. All these mechanisms are designed for digital payment system security.

III. Towards Comparative Analysis Framework of Digital Payment Model

Generally, digital payment is defined as the transfer of money from payer to payee through the use of a digital payment instrument (Korper & Ellis, 2000). Digital payments require exceptional security and trust in the digital business environments (Hai, 2005).

3.1 Review of Digital Payment Model

As we discussed in section 2, credit cards are not only a traditional payment method, but also a well-known digital payment method. In addition, digital cash and digital checks supplement digital payment methods. Each digital payment method has an important role in the digital payment domain. The digital cash method is suitable for small-value

transactions; and the digital checks method is suitable for large-value transactions. The digital credit card method is the most popular digital payment. Table 2 summarizes the issues related to the three types of digital payment methods.

Table 2. Issues on Digital Payment Methods

Payment Methods	Security Provided	Low-value Transaction Support	Privacy (Anonymity)	Applicable Payment Model
Digital Cash	Low to Medium	Yes	Medium to High	Third-party Payment Model
Credit Cards	Low to Medium	No	Low to Medium	Secure Sockets Layer Payment Model / Secure Electronic Transaction Payment Model
Electronic Checks	Low to Medium	No	Low	Simply Encrypted Payment Model

As can be seen from Figure 1, the third-party payment model provides a secure scheme for transaction processing of digital cash (Lawrence & Newton, 2002). The credit card method is based on the secure sockets layer (SSL) payment model and secure electronic transaction (SET) payment model for real-time reliable online payment. The electronic checks method is achieved by applying the digital certificate, digital signature and encryption technique.

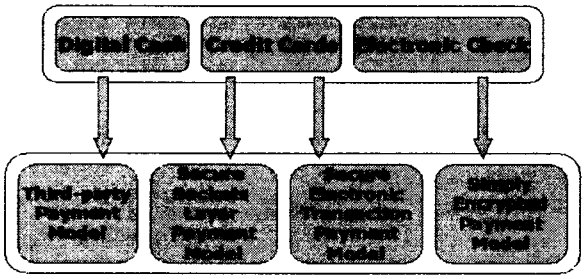

Figure 1. Digital Payment Types & Models

3.2 Comparative Analysis Framework of Digital Payment Models

3.2.1 Overview

Though there are many issues that could affect the security of digital payment transactions, this paper focuses on transaction and system security. This is because these two fields are directly associated to secure digital payment procedure, as can seen from Figure 2.

Based upon the previous overview of the security risks of digital payment, it appears that transaction security is affected by specific and well-defined rules. On the other hand, systems security is influenced by technical infrastructure and implementation (Korper & Ellis, 2000).

Figure 2. Scheme of Secure Digital Payment

1) Transaction Security

Transaction security is thought of as the core of digital transaction security. There are a series of specific rules to ensure transaction security. Transaction security mainly consists of technical details. It provides security measures from digital transaction start to finish, including security of customer account information, security of information delivery, confirmation of customer's validity and so on. Four most important issues are selected to evaluate transaction security: 1) Authentication: prevention of unauthorized parties to capture, interpret or understand data. 2) Privacy (Anonymity): a payment system should prevent disclosure of the identity of the parties to the transaction and it should not be possible to monitor an individual's spending patterns. 3) Refundable: prevention of denying the action of participating in a transaction by a person or entity. 4) Integrity (Encryption): assures that data has not been altered or manipulated by unauthorized parties (Kalakota & Whinston, 1996; Korper & Ellis, 2000; Fajfar, 2004).

According to the above review, it appears that four factors of transaction security should be regarded as major variables for secure digital payment.

2) Systems Security

There are four dimensions of systems security: 1) Hardware security: refers to mechanisms that are used to ensure the security of digital payment transactions. 2) Software security: refers to software that is used for authentication, transaction or communications. 3) Network security: refers to networks for transferring digital payment information. 4) Institution security: refers to institutions such as automated clearinghouse for transaction exchange, certificate authority for verification.

In addition, to ensure system security, it needs to be determined whether digital payment systems are sufficiently secure and should conduct a periodic examination of digital payment systems (Fajfar, 2004).

3.2.2 Comparative Analysis Framework

As discussed above, systems security is divided into four independent variables: hardware security, software security, network security and institution security. Transaction security is also divided into four independent variables: authentication, privacy (anonymity), ability to be refunded and integrity (encryption). Three other important variables are adopted to evaluate the fundamental characteristics of each payment model (Slyke & Belanger, 2003); 1) Transaction cost, 2) Transaction type, 3) and Level of risk. A comparative analysis framework is addressed in Table 3.

Table 3. Comparative Analysis Framework

Comparative Variables / Digital Payment Model		Digital Payment Example
Fields	Variables	
	Hardware Security	

Systems Security	Software Security	
	Network Security	
	Institution Security	
Transaction Security	Authentication Required	
	Privacy (Anonymity)	
	Refundable	
	Integrity (Encryption)	
Transaction Cost		
Transaction Type		
Level of Security Risk		

As can seen from Figure 3, first, we attempt to review four types of secure digital payment model; 1) Simple encrypted payment model, 2) Third-party payment model, 3) SSL payment model, and 4) SET payment model. Second, according to the comparative analysis framework, this paper deals with a comparison of the four digital payment models. Finally, on the basis of research findings so far, a mobile digital payment method is proposed.

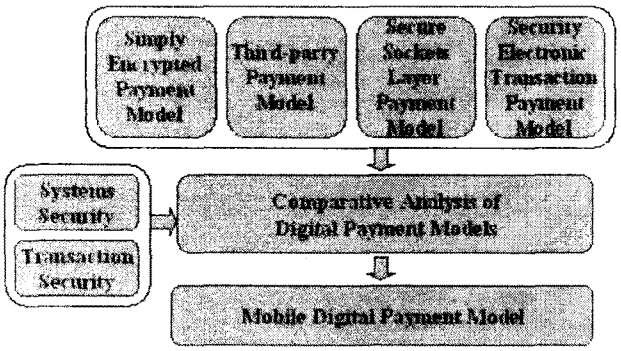

Figure 3. Research Procedure

VI. Comparative Analysis on Digital Payment Models

Based on the previous analysis of three existing popular digital payment methods - digital cash, credit card and electronic checks, a comparative analysis of each model is made, including the flow chart, merits and defects.

4.1 Simply Encrypted Payment Model

1) Flow Chart

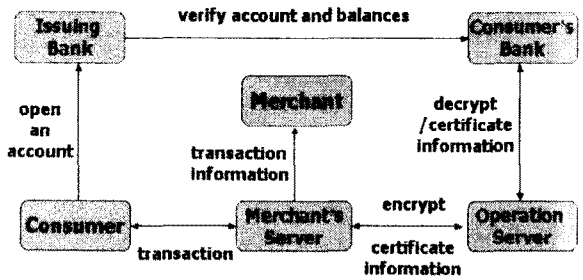

Figure 4. Flow Chart of Simply Encrypted Payment Model

In this model, customers deposit a certain amount of money into a cash server in advance. Then, they obtain corresponding digital cash during the transaction process. The certification server sends acknowledgement information after the customer submits order information to the bank. The information will be encrypted in this model. Adoptive encryption technology includes SHTTP (Bellare & Jutla, 1998). Encrypted information is identified by the service supplier or third-party payment system.

2) Analysis

In this model, important information such as card account numbers should be encrypted during the transaction process, usually using symmetric or asymmetric encryption technology. It is necessary to set up an identity certification system and certify the validity of transaction information using a digital signature (Mantel & McHugh, 2003). An operation server and service software are used for this process. The key in this model is the operation server, which provides a secure transaction environment for ensuring the security of the network. Since the merchant does not know the account information of customer, it is impossible to abuse customer's privacy (Lawrence & Newton, 2002).

4.2 Third-Party Payment Model

1) Flow Chart

In the third-party payment model, the customer opens an account on the third-party's server. During the transaction process, the customer could decide to deposit money into the third-party's server from a bank account, or via other methods. When the customer agrees to pay the merchant, the third-party server transfers money to the merchant's account (Meiqi, 2002).

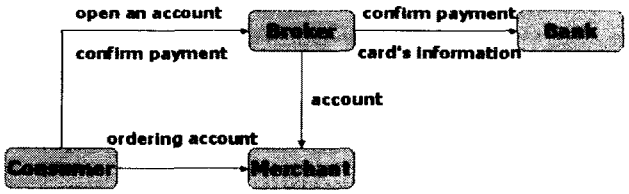

Figure 5. Flow Chart of Third-party Payment Model

2) Analysis

In this model, the account card's information is not transferred over a public network. The customer's identity is confirmed via e-mail. Merchants have a wide range of liberty and low risk. Payment is finished by a third-party (agency), which is trusted by both buyer and seller in the payment transaction. The key of this method is the third-party, so both sides in the transaction process trust the third-party. The risk is assumed by the third-party, which also provides functions such as encryption (Korper & Ellis, 2000).

4.3 Secure Sockets Layer Payment Model

1) Flow Chart

Under the SSL payment model environment, the customer and merchant initially interchange digital certificates with each other. When the secure transfer channel is established between customer and merchant, the

customer sends the ordering information and credit card account to the merchant. Then, the merchant's bank requests validation of the credit card information from the issuing bank. If the information is valid, the issuing bank transfers money to the merchant (Bellart & Garay, 1995; Wright, 2002).

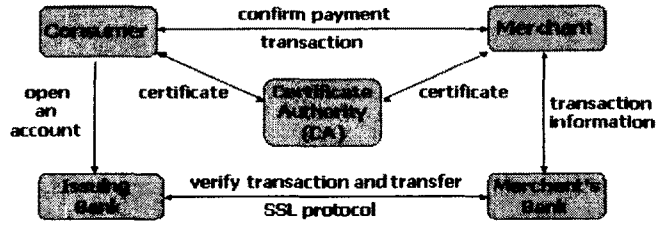

Figure 6. Flow Chart of SSL Payment Model

2) Analysis

The SSL uses the public key/private key encryption system from RSA, which also includes the use of a digital certificate (Mantel & McHugh, 2003). The secure environment for the SSL is created through the use of public key cryptography, which consists of the encryption and decryption of information (Kalakota & Whinston, 1997). Public key cryptography allows anyone to send an encrypted message to a designated recipient, using what is known as a public key. The recipient then uses a private key to decrypt the message. As a result, only the designated recipient has the ability to read the message.

The largest advantage of SSL protocol is for its simplicity. There is also a disadvantage. During the transaction process, the consumer's information is sent to merchants at first. At that time, we can't assure the safety of consumer's information.

4.4 Secure Electronic Transaction Payment Model

1) Flow Chart

Under the SET model environment, the customer opens an online payment account from the issuing bank. The customer downloads the client software from the website of the bank. The customer can also apply a security certificate. During the payment transaction, the customer inputs the user ID, password, validity date and so on. The client software requests certification from the merchant server, then, both the order form and credit card information are sent to the bank through a payment gateway. The payment gateway sends payment acknowledgement information (Meiqi, 2002; Slyke & Belanger, 2003).

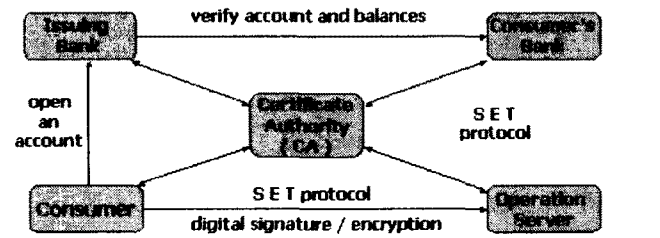

Figure 7. Flow Chart of SET Payment Model

2) Analysis

This model simultaneously uses private key encryption and public key encryption (Lawrence & Newton, 2002). During the transaction process, the validity of customer, merchant and the institution must be identified. The digital signature technique is used to certify the validity of these parties. It is necessary to establish a special certificate authority institution to certify each participant in the transaction (Korper & Ellis, 2000). An electronic envelope is used to assure the security of information transfered. The public key and private key should be changed frequently. SET provides the certification of transaction participants, insuring the transaction data's security and integrity, and particularly ensuring that the account information of a cardholder is not to be released to others (Kalakota & Whinston, 1996).

V. Conclusion and Implications

The comparison results are summarized in Table 4. With the diffusion of digital business, the security of digital payment transactions is becoming more and more important.

Table 4. Synthesis of Digital Payment Model Comparison

Comparative Variables / Digital Payment Model		Simply Encrypted Payment Model	Third-party Payment Model	Secure Sockets Layer Payment Model	Secure Electronic Transaction Payment Model
Fields	Variables				
Systems Security	Hardware Security	No	No	Yes (by Merchant)	Yes (by Merchant)
	Software Security	Yes	Yes	No	Yes
	Network Security	Yes	No	No	No
	Institution Security	Automated Clearing House (ACH)	Certificate Authority (CA)	Certificate Authority (CA)	Certificate Authority (CA)
Transaction Security	Authentication Required	Some/ Digital Certificate, Digital Signature	No	Some/ Digital Certificate, Digital Signature	Good/ Digital Certificate, Dual Signature
	Privacy (Anonymity)	No	Yes	No	Yes
	Refundable (to berepudiated)	Yes	No	No	No
	Integrity (Encryption)	Public Key	Asymmetric Encryption, Public Key	Public Key, Secret Key	Symmetric Encryption, Public Key, Secret Key
Transaction Cost		Low	Low	Low	High
Transaction Type		Large value	Small-value	All types	All types
Level of Security Risk		Low to Medium	Low to Medium	Medium to High	Low

As can be seen from Table 4, the SET payment model provides all-sided security measures. It could be used in both high and low value transactions. However, it's very complex, costs too much and is not suitable for small-value transactions (Kalakota & Whinston, 1996; Hai, 2005). The third-party payment model is popular nowadays. However, its security measures and fund flow are controlled by third-party organizations. Considering the security of funds, it's not suitable for high-value transactions. The simple encrypted payment model is easy to operate. However, it has high costs and is not suitable for small-value transactions.

Based on the previous comparison of four secure digital payment models, this research attempts to propose a mobile digital payment model. In recent years, the significant increasing use of mobile device has caused a strong demand on secured mobile payment services and reliable mobile business applications. Since mobile payment is a critical part of most mobile business applications, the question of how to develop a secured mobile payment model becomes a hot field in both the digital payment field and mobile business area (Antovski & Gusev, 2003; Chou et al., 2004).

With regards to this digital payment circumstance, in this paper, we attempt to propose a mobile digital payment model, which allows mobile users to conduct mobile payment transactions using mobile devices. According to the comparative analysis of previous digital payment models, it appears that a mobile digital payment model is required to synthesize the concept of mobility, wireless payment protocol and mobile digital payment application.

In line with this, the purpose of a mobile payment model aims to provide a convenient and wireless digital payment process. Moreover, mobile payment protocol has to support various mobile consumers to deal with mobile monetary transactions securely. Therefore, a mobile payment protocol model will enable mobile users to conduct mobile payment transactions via wireless networks. At that time, the model should provide a secured protocol, which supports not only the payment transactions between two mobile consumers, but also the secured mobile transactions between the payment server and mobile consumers.

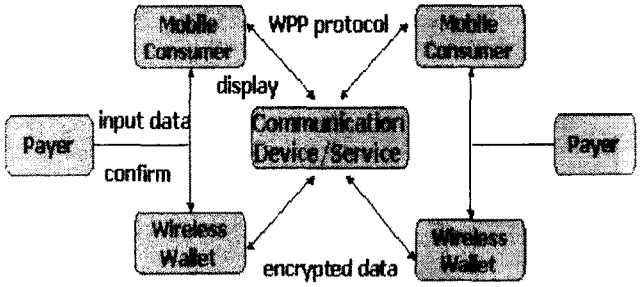

Figure 8. Mobile Digital Payment Model

The mobile digital payment model simplifies the complexity of transaction flow, decreases the number of transaction entities, saves time and money consumption, and makes it easy to implement the mobile payment protocol (WPP). It is hoped that the mobile digital payment model would guarantee a secure transfer of important information and ensure integrity and privacy of transaction information on the basis of both the consumer and the merchant transaction platform.

To sum up, this paper reviews three types of digital payment, and system and transaction security of each digital payment model. Then, we discussed four types of secure digital payment model according to the comparative analysis framework. After that, according to these research results, we propose a mobile payment model, which can simplify the complexity of mobile transaction flow, decrease the number of transaction entities, save time and money consumption, and make it easy to implement WPP protocol. However, this new mobile payment model requires practical application to show its usefulness.

In expanding the boundaries of existing knowledge on digital payment, a number of research agendas can be suggested for the future. First, in focusing on the digital payment comparison model proposed in this research, further research would be necessary to empirically analyze fundamental variables that affect secure digital payment. Second, while the focus of this study is on the comparative analysis of secure digital payment models, further research would be fruitful if it examines a more practical application of the secure digital payment model.

References

[1] Antovski, L. and Gusev, M. (2003). "M-Payments", *Proceedings of the 25th International Conference Information Technology Interfaces.*

[2] Bellart,M. and Garay, J. A. (1995). "iKP — a Family of Secure Electronic Payment Protocols," *Proceedings of the First USENIX Workshop on Electronic Commerce*, New York.

[3] Chou, Y., Lee, C. and Chung, J. (2004). "Understanding M-Commerce Payment System through the Analytic Hierarchy Process," *Journal of Business Research*, Vol. 57, pp. 1423-1430.

[4] Fajfar, M. (2004). "Role and Security of Payment Systems in An Electronic Age," *IMF Institute Seminar on Current Developments in Monetary*, pp. 2-9.

[5] Hai, W. (2004). "Design of Secure Electronic Transaction System," Available at www.paper.edu.cn , pp. 1-5.

[6] Kalakota, R. and Whinston, A. B. (1997). *Readings in Electronic Commerce,* Addison Wesley Publishing.

[7] Laudon, K. C. and Traver, C. G. (2001). *E-Commerce: Business, Technology, Society,* Addison Wesley Publishing.

[8] Lawrence, E., Newton, S., Corbitt, B., Braithwaite, R. and Parker, C. (2002). *Technology of Internet Business,* John Wiley & Sons Australia Publishing.

[9] Mantel, B. and McHugh, T. (2003). "Changing E-payment Payment Networks in The U.S.: The Strategic, Competitive & Innovative Implications," *American Banker*, pp. 8-14.

[10] Meiqi, F. (2002). "Electronic Payment Model," Available at www.xinxihua.cn.

[11] Slyke, C. V. and Belanger, F. (2003). *E-Business Technologies: Supporting the Net-Enhanced Organization,* John Wiley & Sons Inc.

[12] Wright, D. (2002). "Comparative Evaluation of Electronic Payment Systems," *INFOR*, Vol. 40, No. 1, Feb, pp. 71-85.