

# Internet Payment System – Mechanism, Applications & Experimentation

Ka-Lung CHONG

A Thesis Submitted in Partial Fulfilment  
of the Requirements for the Degree of  
Master of Philosophy  
in  
Computer Science & Engineering

Supervised by:  
Dr. Michael R. LYU & Dr. Yiu-Sang MOON

© The Chinese University of Hong Kong  
June 2000

The Chinese University of Hong Kong holds the copyright of this thesis. Any person(s) intending to use a part or whole of the materials in the thesis in a proposed publication must seek copyright release from the Dean of the Graduate School.



論文題目：互聯網付款系統 — 結構、應用及實驗

學生姓名：莊嘉龍

修讀學位：計算機科學與工程哲學碩士

學校：香港中文大學

日期：2000年6月

### 論文撮要：

電子商貿(Electronic Commerce)是運用電信網絡去分享商貿資訊、維持商業機構之間的關係和管理公司業務。隨著電子商貿的流行,各公司都趨之若鶩,在萬維網(World Wide Web)上開設各式各樣的店舖。

互聯網(Internet)上的萬維網成為電子商貿最主要的媒介,令到電子商貿的用途亦極大地擴闊,它的意思亦重新被定義。這個新的媒介更提供一個商業機會給公司做宣傳,不祇是本地,還可讓公司踏出國際市場。除此之外,還可以售賣產品給世界各地的顧客。

同時,互聯網上保安亦是一個熱門的話題。各從事網上商業的機構都在尋求一個保安完善的付款系統(Payment System)去處理聯線的交易。所以,一個保安完善的互聯網付款系統佔去了一個很重要的地位。

在這篇論文中,我提出一個新的互聯網付款系統,它能夠處理顧客、商戶和銀行之間的信用卡交易(Credit Card Payment)。為了幫助測試和評估這個系統,我們開發了一個電子商貿網站名叫 TravelNet。它模擬真實的旅遊代理處,賣機票、旅行用品、旅遊書籍和訂酒店。TravelNet 利用這個付款系統去處理顧客及商戶之間的款項。我們建造了付款系統和 TravelNet 後,同時亦進行了性能評估。評估結果證明了我們的付款系統是簡單易用、安全和合算的。為了使評估有更大的信服力,我們模擬了三個互聯網付款系統(SET, CyberCash, QIPP)與我們的評估結果作比較。模擬結果證明了我們的系統在處理交易時是比較快的。

# Internet Payment System – Mechanism, Applications & Experimentation

submitted by

**Ka-Lung CHONG**

for the degree of Master of Philosophy  
at the Chinese University of Hong Kong

## Abstract

Electronic commerce ( E-commerce ) is the sharing business information, maintaining business relationships, and conducting business transactions by means of telecommunications networks. With the gaining popularity of electronic commerce nowadays, there are many different types of online shop opening in the World Wide Web.

The Internet's World Wide Web ( the Web ) has become the prime driver of contemporary E-commerce, which has been vastly broadened and redefined by the use of the new medium. This new medium provides a business opportunity to companies to advertise themselves not only in a local area, but also anywhere in the world. In addition, the company can sell their products to customers through the World Wide Web.

Meanwhile, Internet security issues become a hot topic and companies accessing the Internet payments are seeking a secure payment system to handle the online transaction. A secure Internet payment system plays a significant role in this online shopping environment.

In this thesis, we propose a new Internet payment system that uses our system server to handle the credit card payment transaction between customers, merchants and banks. To test and evaluate the payment system, we build an online travel agency called TravelNet, which simulates a real-life E-commerce application. Online travel

services including flight reservation, selling of travel accessories, tour guides, and hotel reservation are provided in TravelNet. TravelNet makes use of the proposed payment system to handle the payment transferred between customers and merchants. We implement the payment model as well as TravelNet, and conduct performance evaluation on the payment system. The performance results show that our payment system is easy-to-use, secure, and cost-effective. To improve the creditability of our performance evaluation, we simulate three existing payment systems ( i.e., SET, CyberCash and QIPP ) to compare with our performance evaluation on our payment model. The simulation results showed that our model completed a transaction in a short period of time when compared with other systems.

## Acknowledgments

I would like to thank my supervisors, Dr. Michael R. Lyu and Dr. Yiu-sang Moon, for their kindness, invaluable advice, commitment, guidance as well as assistance throughout this research project.

Besides, I am sure, this thesis reflects the love and support provided by my parents throughout my life; they have given me more than is imaginable.

My friends, Ka-po Ma, Siu-chung Ng, Kai-kai Tsai, Kam-lai Wong, Hing-wing Chan, Kwong-wai Chen, Po-shan Kam, Wing-kai Lam, Tsui-ying Law, Wai-ching Wong and Wai-chiu Wong, I thank them for giving me fun and support.

Finally, I wish to acknowledge the influence of my girl friend, Tina Lai-yuk Lam. The joy, encouragement and spiritual support she has given me are immeasurable.

# Contents

<b>Abstract</b>	<b>i</b>
<b>Acknowledgments</b>	<b>iii</b>
<b>1 Introduction &amp; Motivation</b>	<b>1</b>
1.1 Introduction . . . . .	1
1.2 Internet Commerce . . . . .	3
1.3 Motivation . . . . .	6
1.4 Related Work . . . . .	7
1.4.1 Cryptographic Techniques . . . . .	7
1.4.2 Internet Payment Systems . . . . .	9
1.5 Contribution . . . . .	16
1.6 Outline of the Thesis . . . . .	17
<b>2 A New Payment Model</b>	<b>19</b>
2.1 Model Description . . . . .	19
2.2 Characteristics of Our Model . . . . .	22

2.3	Model Architecture . . . . .	24
2.4	Comparison . . . . .	30
2.5	System Implementation . . . . .	30
2.5.1	Acquirer Interface . . . . .	31
2.5.2	Issuer Interface . . . . .	32
2.5.3	Merchant Interface . . . . .	32
2.5.4	Payment Gateway Interface . . . . .	33
2.5.5	Payment Cancellation Interface . . . . .	33
<b>3</b>	<b>A E-Commerce Application – TravelNet</b>	<b>35</b>
3.1	System Architecture . . . . .	35
3.2	System Features . . . . .	38
3.3	System Snapshots . . . . .	39
<b>4</b>	<b>Simulation</b>	<b>44</b>
4.1	Objective . . . . .	44
4.2	Simulation Flow . . . . .	45
4.3	Assumptions . . . . .	49
4.4	Simulation of Payment Systems . . . . .	50
<b>5</b>	<b>Discussion of Security Concerns</b>	<b>54</b>
5.1	Threats to Internet Payment . . . . .	54
5.1.1	Eavesdropping . . . . .	55
5.1.2	Masquerading . . . . .	55



5.1.3	Message Tampering . . . . .	56
5.1.4	Replaying . . . . .	56
5.2	Aspects of A Secure Internet Payment System . . . . .	57
5.2.1	Authentication . . . . .	57
5.2.2	Confidentiality . . . . .	57
5.2.3	Integrity . . . . .	58
5.2.4	Non-Repudiation . . . . .	58
5.3	Our System Security . . . . .	58
5.4	TravelNet Application Security . . . . .	61
<b>6</b>	<b>Discussion of Performance Evaluation</b>	<b>64</b>
6.1	Performance Concerns . . . . .	64
6.2	Experiments Conducted . . . . .	65
6.2.1	Description . . . . .	65
6.2.2	Analysis on the Results . . . . .	65
6.3	Simulation Analysis . . . . .	69
<b>7</b>	<b>Conclusion &amp; Future Work</b>	<b>72</b>
<b>A</b>	<b>Experiment Specification</b>	<b>74</b>
A.1	Configuration . . . . .	74
A.2	Experiment Results . . . . .	74
<b>B</b>	<b>Simulation Specification</b>	<b>77</b>

B.1 Parameter Listing . . . . .	77
B.2 Simulation Results . . . . .	77
<b>Bibliography</b>	<b>80</b>

# List of Tables

1.1	A Summary of Comparisons between Different Internet Payment Systems	16
2.1	Notations Used in the Message Content of Payment System . . . . .	25
2.2	A Comparison between Our Payment Model and Different Internet Payment Systems . . . . .	30
A.1	Experiment Result of ‘Payment Transaction Time in Multiple-Threaded Model’ . . . . .	75
A.2	Experiment Result of ‘Payment Transaction Time in Single-Threaded Model’ . . . . .	75
A.3	Experiment Result of ‘A Comparison for Single-Threaded and Multi-Threaded Model’ . . . . .	76
A.4	Experiment Result of ‘Single-Threaded Model on the Payment Transaction Time on PG’ . . . . .	76
B.1	Parameters Used in Simulation . . . . .	78
B.2	Parameter Values Used in the Simulation . . . . .	78
B.3	Result of SET, CyberCash and QIPP Simulation . . . . .	79
B.4	Result of Comparison between Our System, SET, CyberCash and QIPP Simulation . . . . .	79

# List of Figures

1.1	Architecture of SET Protocol . . . . .	11
1.2	Architecture of Secure Socket Layer Protocol . . . . .	12
1.3	Architecture of CyberCash Payment System . . . . .	13
1.4	Architecture of Qudro-way Internet Payment Protocol . . . . .	15
2.1	Flow Diagram of an Online Transaction . . . . .	20
2.2	Our Payment Model and Its Payment Process Flows . . . . .	26
2.3	System Flow Diagram of Our Payment Model . . . . .	29
3.1	Overall Architecture of TravelNet . . . . .	36
3.2	Main Page of TravelNet . . . . .	40
3.3	Flight Search Screen . . . . .	42
3.4	Check-Out Screen . . . . .	43
3.5	Transaction Completion Screen . . . . .	43
4.1	Flow Diagram of the Simulation . . . . .	46
4.2	Interaction between Different Entities in the Simulation Model . . . . .	48
6.1	Payment Transaction Time in Multiple-Threaded Model . . . . .	67

6.2	Payment Transaction Time in Single-Threaded Model . . . . .	68
6.3	A Comparison for Single-Threaded and Multi-Threaded Model . . . . .	68
6.4	Single-Threaded Model on the Payment Transaction Time on PG . . . . .	69
6.5	Simulation of SET, CyberCash and QIPP . . . . .	70
6.6	A Comparison between Our System, SET, CyberCash and QIPP . . . . .	71

# Chapter 1

## Introduction & Motivation

### 1.1 Introduction

With the advances in information technology and networking, Internet commerce provides a new channel for business advertising, a direct communication of selling products from companies to customers, a direct and faster response from customers to companies. This technology advancement made a tremendous impact on everyone's life as well as the operations of companies.

The impact on everyone's life was from the booming of the Internet. Due to the advancement in computer technology moved faster than ever expected, the cost of a computer set<sup>1</sup> dropped quickly after a period of time; therefore, more people can afford a computer easier than the past few years. Computer became a necessary product rather than a luxury product to a person. More computers are connected together and form a new virtual society in the Internet. People can access there using their computers, go to the virtual shopping mall for buying clothes; go to the virtual campus for self-studying; go to the virtual restaurant for eating; travel around the world; and read the daily news from anywhere in the world, etc.; in simple words, the Internet breaks the physical barriers of time and space, via the World Wide Web ( the Web ), people can get any information there.

---

<sup>1</sup>The computer set contains the basic configuration of a computer for a computer novice who can perform the functions such as connecting to the Internet and doing word-processing.

With the booming of the Internet, it provides a new medium for advertising and selling of company's products. Those business activities can be held in the Web. Besides, it also provides a new type of business environment such as bidding, to be held in the Web. The Web is a big potential market because different market segments such as different age group of people and different professionals can be found. Therefore, the Web provides a new medium for advertising the company and provides a direct selling of products to customers without the middle party – wholesaler; thus, the capital of a company will decrease.

Moreover, company computers can communicate with computers in other companies in exchange of standardized electronic transaction documents. This practice is called Electronic Data Interchange ( EDI ) [19], which is a type of Electronic Commerce ( E-commerce ).

Quote from N. R. Adam and Y. Yesha's book [2],

... E-commerce is defined as the entire set of processes that support commercial activities on a network and involve information analysis. These activities spawn product information and display events, services, providers, consumers, advertisers, support for transactions, brokering systems for a variety of services and actions ( e.g., finding certain products, finding cheaply priced products, etc. ), security of transactions, user authentication, etc., ...

Another quote from the Electronic Commerce Innovation Centre [4] defined E-commerce,

... It involves "the enablement of a business vision supported by advanced information technology to improve efficiency and effectiveness within the trading process." ...

By the first definition of E-commerce, it gives out a clear understanding of a broad definition; commercial activities on a network are considered as E-commerce. From



the second definition, it states out the goal of E-commerce. In other words, it reduces product and service cost, while it improves customer response time and quality. Hence implementing initiatives in electronic commerce has emerged as a significant business strategy in the Information Age.

E-commerce is a multidisciplinary field that includes technical areas such as networking and telecommunication, security, storage and retrieval of multimedia; business areas such as marketing, procurement and purchasing, billing and payment, and supply chain management; and legal aspects such as information privacy, intellectual property, taxation, contractual and legal settlements.

The Internet can be a formidable new channel to attract new customers, transact business with them, to communicate with them and retain them as customers by supporting them. By using the Internet for electronic commerce, businesses can link more of their core processes to their suppliers and customers, extending their reach, bolstering their competitiveness, speeding time to market and fostering customer loyalty. Therefore, the company can utilize this new technology to have competitive advantage over other companies. Many companies are building commerce systems in the Web because they see this approach as a way to accelerate their ability to respond to changes in the marketplace and improve their time to market with new solutions. Many are achieving impressive results by combining the Internet with the power of existing Information Technology applications and data.

## **1.2 Internet Commerce**

The Internet has become the driver for E-commerce thanks to the invention of the Web as a principal means of sharing information and of the browser as the universal front end. The Web has turned the Internet into a global, distributed, and hyperlinked multimedia database. By relying on the client/server architecture, the Web further builds on the decentralized model of the Internet. It is easy to join and it is easy to organize an information space for a small or a very large group. Internet communities



can carve out and shape the space that suits their purposes [3]. The Web can serve as a medium for presentation, distribution, and use-based sale of passive or active ( in the sense of software ) information objects. Specialized platform-independent programming languages, such as Java, facilitate making the electronic pages of the Web into a source of active software objects. It needs to be seen clearly that, as a separate and software-based layer, the Web can and may be replaced in the future by an information management mechanism that would better meet the demands of very-large-scale use of the global network of networks.

Internet commerce ( I-commerce ) is but one type of the more general “Electronic Commerce”. By I-commerce, we mean the use of the global Internet for purchase and sale of goods and services, including service and support after the sale. The Internet may be an efficient mechanism for advertising and distributing product information. Nowadays, many companies are building web pages to distribute their product information as well as turning the Internet as a buying place for the customers.

However, in order to handle a transaction made in the Web, we have to define the money used in the Web and a complete payment system to handle it. In the Web, the most often money used in the transaction are electronic cash and credit card. Unlike physical money, electronic cash is merely bits, and thus can be trivially duplicated. The customers first use their physical money in exchange of the electronic cash, and then they can use the electronic cash to purchase goods in the Web. The other way is to use credit card, however, without a secure and complete payment system to support, the credit card information can be stolen by an intruder. Therefore, we can see the importance of a secure payment system and his playing role in an insecure environment.

Four major elements are associated with payment systems:

- the parties involved;
- the means of payment;
- the medium of exchange; and

- the infrastructure handling transactions.

The parties involved can range from banks or financial institutions, individuals, non-bank corporations, to computer software providers. The means of payment include currency, credit and bank deposit. The medium of exchange includes cash, credit cards, checks, or bills. The infrastructure handling the transaction can be ATMs<sup>2</sup> and POSs<sup>3</sup>, check and bill clearing systems, and Internet banking. These elements are common to most of the payment systems.

For the transactions performed in Internet in an electronic form, we need a secure Internet payment system to handle the transactions. The following criteria should be considered when an Internet payment system is introduced:

- **Security:** The major concern in the payment system used in the Internet is security. As the communication networks are not secure enough, intruders can steal personal information from customers and make use of the information illegitimately. To prevent fraud and disputes, the system should incorporate entity authentication of the parties, message integrity protection, and non-repudiation of payment order. The number of parties involved in the payment process is also a factor to affect the security of the system.
- **Cost:** The revenue of payment orders should be larger than the expense of the payment system. Cryptography is used to encrypt critical information before it is transmitted to the network. A complex cryptographic algorithm at a higher cost achieves higher security. As a result, higher security is used only for higher transaction cost as the cost for complex cryptography algorithms can then be justified.
- **Time:** The time of the payment process should be reasonably fast so that customers are not kept waiting impatiently. The efficiency of the payment system, on the other hand, depends on the computation time of the cryptographic al-

---

<sup>2</sup>ATM is the short form of Auto Teller Machine.

<sup>3</sup>POS is the short form of Point of Sales terminal.

gorithm, the payment mechanism, and the number of parties involved in the payment process.

- **Capacity:** The capacity of the system is regarding the number of people who can use it concurrently. In other words, it refers to the maximum number of people who can use the system for online purchase without system failure due to overloading.

With the support of a secure payment system fulfilling the previous criteria, the customer will purchase online in the Web with less security threats in losing their personal information.

### 1.3 Motivation

Editors of the National Geographic Traveler Magazine [10] elect Cyberspace to be one out of fifty places that travelers should visit in their lifetime. They conclude that Cyberspace is one of the world wonders and a place easy to access for travelers. Despite of this, a secure environment can attract more people to purchase products in the Web.

Consumer-oriented E-commerce is significantly lagging behind its business-to-business segment and current estimates place it at less than 10 percent of the total volume. The settlement phase of transacting on the Web is often pointed to as one of the limiting factors. The consumer should be able to pay for a purchase on the Web easily and with a perception of security. The overall shopping experience, product perceptions, and customer service on the Web today lead to a dissatisfaction of potential customers [16]. From the recent survey conducted by *iamasia* [15], they found that only 15 percent of Internet users in Hong Kong that have purchased online, which the total number of Internet users is about 1.85 million. They lack of confidence on purchasing online accounts for only a small percentage of people have purchased online.

There are many Internet payment systems nowadays, however, one of the problem is they target at different markets, small-valued transaction or large-valued transaction,



that waste the effort of developers. Besides, the basic cost of each transaction is large enough due to the usage of complicated cryptographic tools and authorization of different parties. Most parties have to be online to handle the transactions, so the cost will be increased. Based on the previous points, we design a new payment system to gain satisfaction from the customers and to ameliorate the previous weak points. We build a secure Internet payment system incorporated into the merchant web server and provide an interface for communicate with the bank to complete the transaction. In this thesis, we present the mechanism of our payment model, discuss the differences when compared with other payment systems, how to incorporate it into an E-commerce application – TravelNet ( we will discuss TravelNet in Chapter 3 on page 35 ), and conduct experiments on testing and evaluating our payment model.

## 1.4 Related Work

### 1.4.1 Cryptographic Techniques

Cryptography is useful in protecting against a wide variety of other attacks on the communications between two parties over the computer networks. The art of protecting information by transforming it ( encrypting it ) into an unreadable format called ciphertext. Only those who possess a secret key can decipher ( or decrypt ) the message into plaintext.

#### Symmetric Key Algorithm

For symmetric key algorithm, known as secret-key algorithm, encryption and decryption key are the same and must be kept secret. Symmetric key systems are simpler and faster than asymmetric key ( public-key ) systems, but their main drawback is that the two parties must somehow exchange the key in a secure way.

Symmetric algorithms can be divided into stream ciphers and block cipher. Stream ciphers can encrypt a single bit of plaintext at a time, whereas block ciphers take a

number of bits ( typically 64 bits in modern ciphers ), and encrypt them as a single unit.

The most popular symmetric-key system is the Data Encryption Standard ( DES ) [27, 28] developed in 70s. DES is a block cipher with 64-bit block size. It uses 56-bit key. With this key length, DES is considered as unsafe for the future use. There is a variant of DES, Triple-DES or 3DES. It is based on using DES three times ( in an encrypt-decrypt-encrypt sequence with three different, unrelated keys ).

### **Asymmetric Key Algorithm**

Unlike secret key algorithms, public key algorithms use a different key for encryption and decryption. The decryption key cannot ( practically ) be derived from the encryption key. The merit of public key algorithms is that they can be used to transmit encryption keys or other data securely even when the parties have no opportunity to agree on a secret key in private.

Public-key system gains popularity in the cryptography field than symmetric-key system. It is because the public-key system achieves both secrecy and authenticity while the symmetric-key system achieves secrecy only. The other reason is that public-key system eliminates the problems of distributing key to users. However, public-key system incurs key management and computing overhead problems. A wellknown, widely used public-key system is RSA public-key system [33]. Three scientists: Ron Rivest, Adi Shamir and Leonard Adleman developed it in 1977. This public-key cryptosystem offers both encryption and digital signatures ( authentication ). It is generally considered to be secure when sufficiently long keys are used.

### **Digital Signature**

It is used to detect unauthorized modifications to data and to authenticate the identity of the user who generates the signature. In addition, the recipient of signed data can use a digital signature in proving to a third party that the signature was in fact

generated by the signer of the data. This is known as non-repudiation since the signer of data cannot repudiate the signature at a later time. There is a standard called Digital Signature Standard ( DSS ) and it specifies a Digital Signature Algorithm ( DSA ), which can be used to generate a digital signature.

### **Message Digest**

It is the representation of text in the form of a single string of digits, created using a formula called a one-way hash function. Encrypting a message digest with a private key creates a digital signature, which is an electronic means of authentication. In order to avoid intruder attach any false message onto any other person's valid message or signature, it should not be possible to find two or more than two messages that hash to a same value.

### **Public-key Certificate**

It is a data structure used to securely bind a public key to attributes, which are the identification information such as name, permission. A standard for identification is contained within the international standards for directories such as X.509 certificate binds a public key to a directory name.

## **1.4.2 Internet Payment Systems**

There are many wellknown protocols working in the Internet nowadays. Feature likes pre-registration of user, is always required in most payment systems. Online credit card payment is the usual approach to deal with Internet payment. Its information or account PINs <sup>4</sup> will be transmitted to the merchant or bank over the insecure network. Another approach is electronic coin system. By using this approach, the customer will first buy the electronic coins from the bank either by cash or by credit card. Then they can use electronic coins in online purchasing.

---

<sup>4</sup>PIN is the short form of Personal Identification Number.

For credit card payment, there are many Internet payment systems handling this approach. The first system is First Virtual ( FV ) [30]. It was launched in October 1994. The philosophy of this system is “try before you buy”. This special philosophy accounts for a long time lag between delivering products and capturing of payments. However, First Virtual was defunct now. We continue to discuss other payment systems.

## **iKP**

Internet Keyed Protocol ( iKP ) [11] has been proposed by IBM. It is an online payment system applying Certificate Authority based ( CA-based ) security. The iKP can be implemented in different level, just as its name indicated, iKP (  $i = 1, 2, 3$  ). Different level of iKP offers different security level. The 1KP does not provide non-repudiation; the 2KP provides only non-repudiation of messages produced by merchant; the 3KP achieves non-repudiation for all messages and parties involved. In the iKP, the authorization of payment is based on the credit card number and associated PIN. The PIN will be encrypted with the public key of the acquirer, so that the merchant will have no chance to abuse the credit card of the customer. The iKP assumes that the PIN is not of necessity in these circumstances, since the signature of the customer already offers protection for the account of the customer. There is also iKP for micropayment [14].

## **Secure Electronic Transaction**

Secure Electronic Transactions ( SET ) [22], a protocol for securing electronic payments which protects payment information among users, merchants, and banks. SET was incorporated by MasterCard and Visa; it mainly deals with their branded credit cards. It images electronic commerce built on the CA-based security. Figure 1.1 shows the architecture of SET protocol. It illustrates the importance of certificate authority, serves as trust third party to authenticate different parties. The SET applies acquirer payment gateway that is able to authorize using the existing bankcard networks. In the authorization request sent by merchant to acquirer, the purchase instruction of customer enables the acquirer to verify that the merchant and customer agree as to



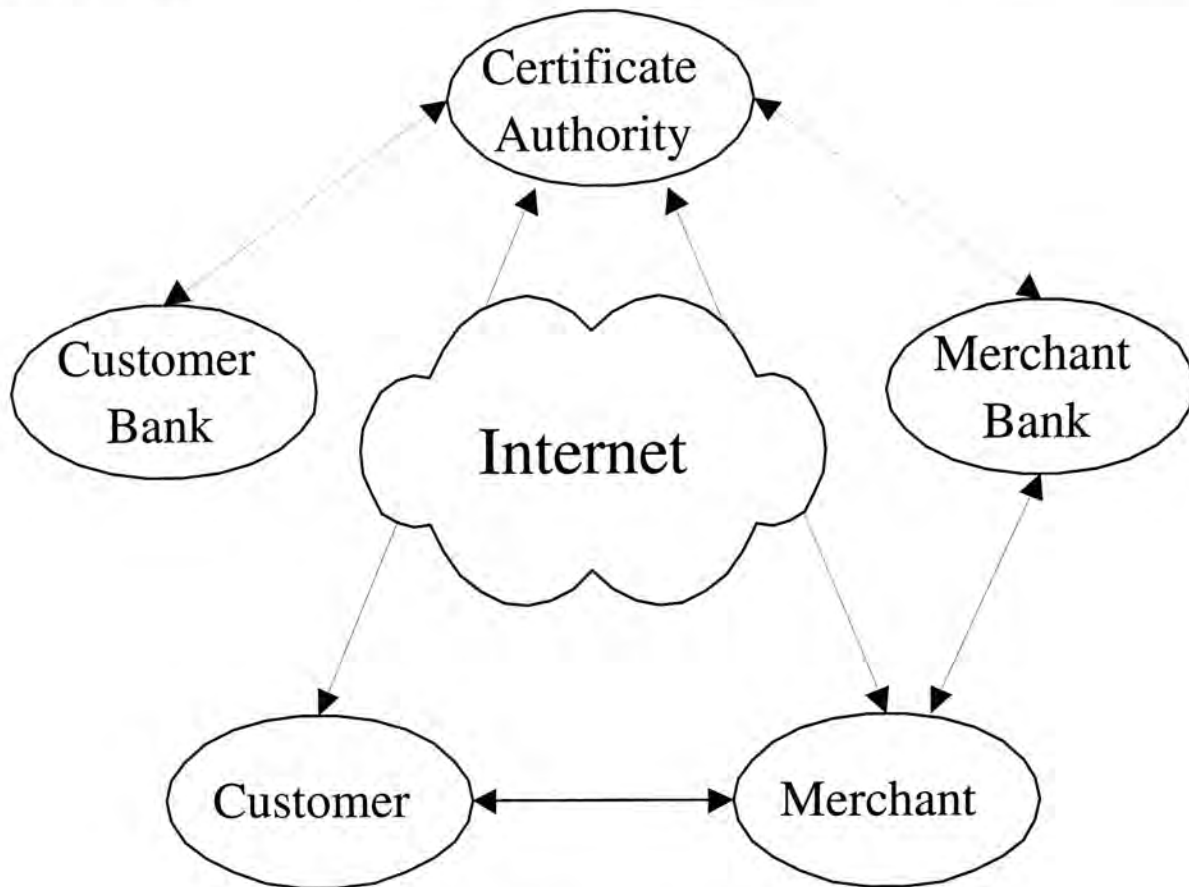


Figure 1.1: Architecture of SET Protocol

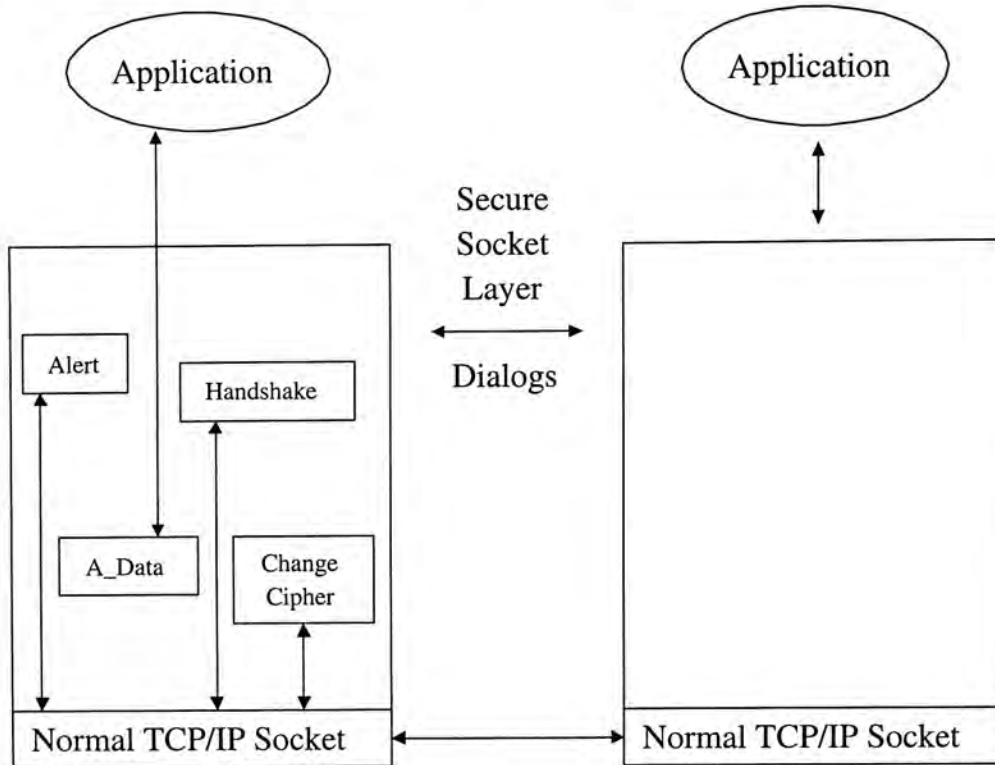
what was purchased and how much the authorization is for.

The SET is a wellknown secure electronic commerce payment protocol nowadays where there are five parties ( customer, merchant, payment gateway ( it is the same as acquirer ), certificate authority and issuer ) involved in the payment process. However, since there are five parties involved and there are much computation times on making signature and encrypting as well as verifying the signature and decrypting the cipher message. Although SET is secure for making electronic transaction online, it is not recommended to work with micropayment because it is too time-consuming and the parties have to authenticate themselves.

### Secure Socket Layer

Secure Sockets Layer ( SSL ) [13] is a session-layer protocol used on the Web to protect credit card numbers and other sensitive data transmitted between a user's browser





**Figure 1.2:** Architecture of Secure Socket Layer Protocol

and an Internet web server through the HyperText Transport Protocol ( HTTP ); and Secure HTTP ( S-HTTP ), which integrates encryption into the HTTP protocol. SSL was developed by Netscape Communications Corporation. Figure 1.2 shows the architecture of SSL protocol. The SSL Handshake Protocol allows the server and client to authenticate each other and to negotiate an encryption algorithm and cryptographic keys before the application protocol transmits or receives its first byte of data.

One advantage of SSL is that it is application protocol independent. A higher level protocol can layer on top of the SSL Protocol transparently. For online communication, SSL allows traffic between a Web server and client ( i.e., the browser ) to be strongly encrypted, using public-key technology. There is one major disadvantage when compared with SET Protocol doing online electronic transaction, SSL cannot prevent the personal information being stolen in transit as well as the merchant being able to examine or tamper with them. Comparisons between SET and SSL can be found in [26].

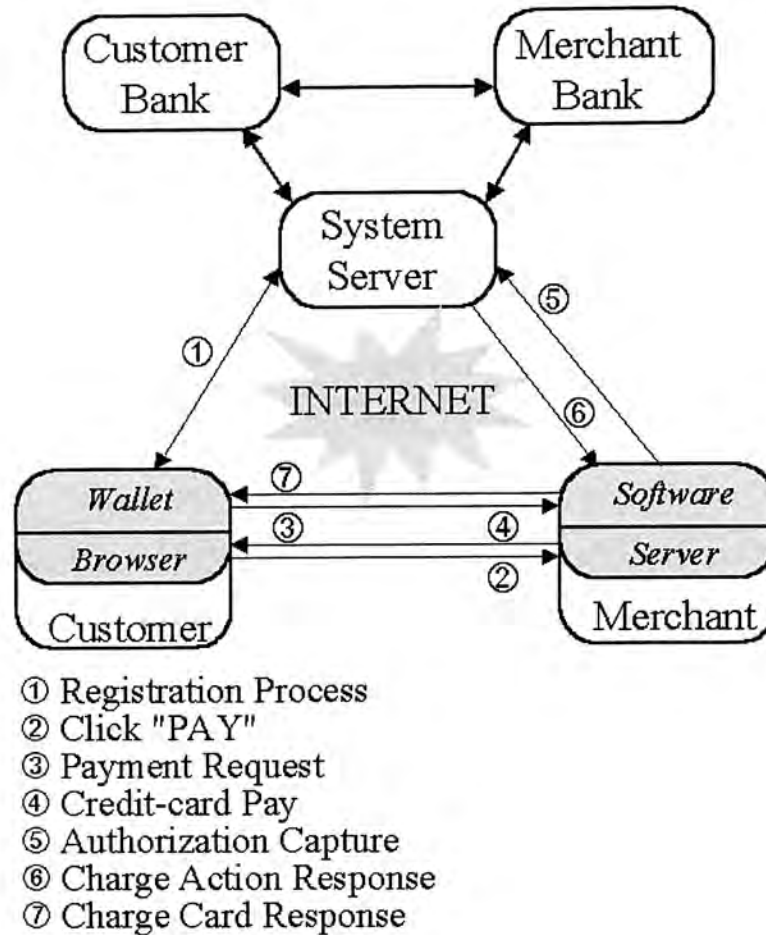


Figure 1.3: Architecture of CyberCash Payment System

## CyberCash

CyberCash [1, 7] founded in 1994, is a pioneer in electronic commerce software and services for merchants. The company offers a unique and wide range of software and service solutions for payment processing, for both Internet and physical store retailers. This allows CyberCash to provide solutions for payment processing that comprise both state-of-the-art services operated by a sophisticated operations center and robust software that can be managed by the merchant customer. CyberCash developed two software applications: one is for credit card payment and the other is called CyberCoin, for electronic coin payment.

Figure 1.3 illustrates the architecture of CyberCash payment system. The architecture is similar as the SET protocol. Special software is needed in customer's computer

in order to purchase online from a shop using CyberCash as the payment system. Once you have installed the wallet software, it will help you to transmit your credit card information to merchant web server automatically while you finish ordering the goods.

### **Qudro-way Internet Payment Protocol**

Qudro-way Internet Payment Protocol ( QIPP ) [41] is a simple yet secure electronic payment for the electronic market on the Web. The Protocol imitates the conventional payment in a shop. There are four parties involved: customer, merchant, payment gateway and certificate authority. Figure 1.4 shows the architecture of QIPP protocol. It is different from other payment systems, the customer will initiate the payment, and the merchant is not directly involved in the payment process. One benefit is observed that the merchant is virtually excluded from the attacks towards account of customer at that bank.

### **DigiCash**

The DigiCash [6] is invented by Belgian-based US cryptographer David Chaum. It uses public-key cryptography techniques to assure anonymity and it is an online electronic cash system. The DigiCash system aims to provide the privacy of customers, based on blind signature [5]. When the customer consumes digital cash, the DigiCash multiplies the note number by a random factor and sends it to the bank for signing. Thus, the bank knows nothing about what it is signing except that it carries customer's digital signature. After receiving the blinded note signed by the bank, the customer divides out the blind factor and uses the note as before. The blinded note numbers are unconditionally untraceable. That is, even if the shop and the bank collude, they cannot determine who spent which notes. Because the bank has no idea of the blinding factor, it has no way of linking the note numbers that a merchant deposits with customer's withdraws. The anonymity of blinded notes is limited only by the unpredictability of customer's random numbers. However, there is a problem that the bank has to keep track of the used digital cash so as to prevent double spending and the database will

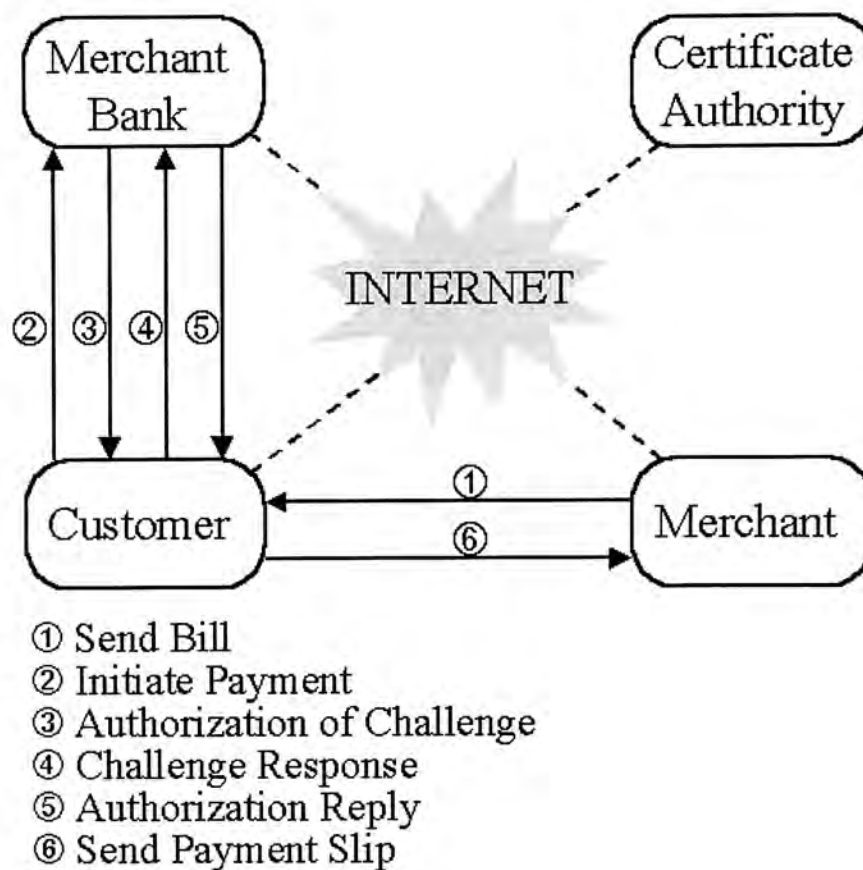


Figure 1.4: Architecture of Quadro-way Internet Payment Protocol

grow enormously and quickly. This greatly affects the performance of the system.

### NetCash

NetCash [23, 24] is a framework for electronic cash developed at the Information Sciences Institute of the University of Southern California. It uses identified online electronic cash. Although the cash is identified, there are mechanisms whereby coins can be exchanged to allow some anonymity. The system is based on distributed currency server. The use of multiple currency servers allows the system to scale well. Disadvantages of the system are that it uses many session keys and in particular public key session keys. In a transaction, a buyer uses NetCash coins to purchase an item from a merchant. The buyer remains anonymous since the merchant will only know the network address of where the buyer is coming from.

	<b>Payment Options</b>	<b>Cryptography level</b>	<b>Anonymous</b>
CyberCash	credit card & e-cash	high	no
QIPP	credit card	intermediate	yes
SET	credit card	high	yes
SSL	credit card	intermediate	no
DigiCash	e-cash	low	yes
NetCash	e-cash	low	yes

**Table 1.1:** A Summary of Comparisons between Different Internet Payment Systems

In Table 1.1, we summarize the characteristics of different Internet payment systems.

There are many other payment protocols which some is a collection of the successful parts from existing systems, minus the failings of those systems. They choose those strengths and neglect those weaknesses. For example, the PayMe system [29] is based on a close examination of systems such as NetCash, Ecash and other related systems such as Magic Money [8] and Netbill [36, 39]. PayMe system preserved as much of the anonymity provided by Ecash while adopting many of the features of NetCash that allow it to scale to large numbers of users with multiple banks. Moreover, other payment protocols such as Millicent [25], PayWord and MicroMint [32], which are also wellknown.

## 1.5 Contribution

The contribution of this research project is building a secure Internet payment system that the merchant can incorporate our system into their web server easily. The merchant web server makes a call to the software we provided to establish a secure channel to transmit confidential information to our payment system. Small amount of effort is needed to the merchant to use our software.

Besides, our payment system can support not only one payment method, but also



few more payment methods. By plugging the specific component software to our system, it can handle the specific payment method. We have designed our system to check which payment method the customer chose during online purchasing.

After we integrate our payment system into TravelNet, TravelNet becomes a complete e-commerce online travel agency. It can handle transactions from worldwide customers.

Moreover, we conducted several experiments to evaluate the performance of our payment system. Also, we built three computer models of existing payment systems, SET, CyberCash, and QIPP, to simulate their performance. The parameters used make the simulation models more realistic.

## **1.6 Outline of the Thesis**

In this chapter, I introduced what Internet commerce was, how it provided a new place for company to distribute their product information, what the importance of a secure payment system is nowadays as there are increasing number of companies building systems in the Internet. I discussed some existing Internet payment systems and a summary was drawn in comparing between different payment systems.

In chapter 2, I will present our payment model. What is our model? What are the merits and deficits of our model? What are the architecture and the message flow of our model? Who are our targets? How did we implement our model? Those queries will be solved in that chapter.

In chapter 3, I will discuss an E-commerce application called TravelNet, is a project that simulates a real life an online traveling agency. Our model helps to handle the payment transaction of TravelNet. I will discuss the architecture and features of TravelNet, shows the system snapshots including the moment of processing payments.

In chapter 4, I will simulate three other Internet payment systems and compare with our model. The three simulated systems are SET, CyberCash and QIPP. What

---

are the simulation results? What are the differences between those systems and ours? Those answers can be found in that chapter.

In chapter 5, I will discuss the threats to Internet payments. How will the threats influence payments over the network? Hence, I describe the aspects of a secure Internet payment system. I will discuss in details how secure of our system as well as the completed E-commerce application, i.e., our payment model incorporated into TravelNet.

In chapter 6, I will present the experiment on testing our model and the combined system, i.e., TravelNet and our model. Then we will present the experiment results and the simulation results. How were the experiments conducted and what are the assumptions of the simulation?

Finally, in chapter 7, it is a conclusion on revisiting all the important points in this thesis. Other additional information, the configuration and the results of simulation, and the configuration and the results of experiments can be found in Appendix.

## Chapter 2

# A New Payment Model

In this chapter, we present a new payment model ( our model ). We first describe our model. Then we discuss the characteristics of our model, the merits and the deficits of our model. Next, we present the architecture of our model together with the notations used throughout this thesis in describing the message contents. We illustrate our model in the communication between customer, merchant and bank. Then, we present a comparison of our model to the other three payment systems ( SET, CyberCash and QIPP ) presented in Section 1.4.2 on page 9. Finally, we present the implementation of our model.

### 2.1 Model Description

In this section we propose a new Internet payment system. The proposed system resembles the buying steps of a customer who uses a credit card or cash card to purchase goods. The procedure of purchasing online in our payment system is the same as that in a real life.

The system provides a credit card payment method. Customers must own a credit card in order to make online transactions. The conventional shopping choice is preserved. Figure 2.1 illustrates the flow of an online transaction.



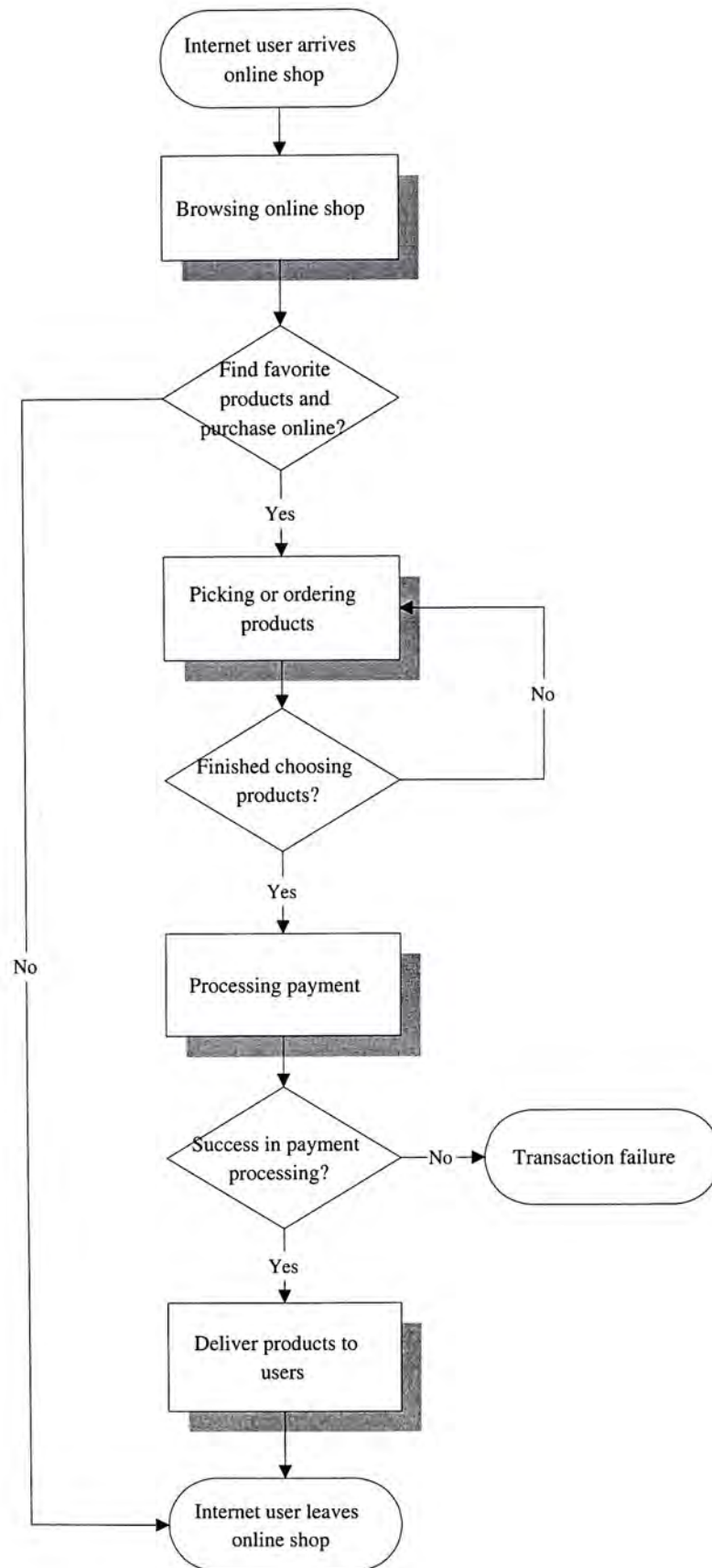


Figure 2.1: Flow Diagram of an Online Transaction

The payment algorithm is as follows:

1. Customer who likes to purchase online must own at least one credit card, which has enough credit amount inside.
2. The customer browses the online shop that is using our payment system to handle online transactions.
3. When the customer finishes choosing the products, he will initiate the payment process. The process will be transparent to the customer.
4. The merchant web server will call our software resided there to connect to our payment system. Confidential data such as customer credit card information will be passed to our payment system using a secure channel using cryptographic techniques.
5. Our system will send the payment request to corresponding bank system to complete the request.
6. Our payment system will send a positive acknowledgment to the merchant web server upon the receipt of the corresponding banking system.

The details of each payment procedure and the message used will be discussed in Section 2.3.

Our target users are merchants who seek for a payment system with less modification to their web pages and Internet users who primarily work at home and stay beside a network-connected computer to the Internet.

There are four major entities involved in our system. They are customers, merchants, a payment gateway and banks. The Certificate Authority will manage the certificate and those public keys required for the entities. RSA public-key cryptography is used for authentication and encryption purposes. A pair of private/public keys is generated by the customer or by a trusted third party, i.e., the Certificate Authority.

Our main focus is on the purchasing part ( how customers interact with merchants ) and the payment process ( how money is settled down ). Other traditional security issues such as how the keys will be managed and distributed to the users are not our major concern. Besides, there is a general assumption that it is secure from attacks in the communications network between the payment gateway and the existing banking system.

Our payment system acts as a gateway to the banking systems. It is a private entrance to the banking systems. That is a merchant without using our provided software; merchant cannot utilize our payment system to connect to the banking systems. A small-sized software component will be resided in the merchant web server so that merchant can send confidential data of customer to the corresponding bank for verification and payment authorization.

Therefore, we can divide our system into two parts: one is the main system, to handle the requests from merchant and to request banks for either payment authorization or payment cancellation; the other one is for the use by merchant web server.

## 2.2 Characteristics of Our Model

Our model provides a number of features as follows:

- Give choices on payment method
- Avoids threats <sup>5</sup> attack;
- Easy to use;
- Easy to incorporate into a merchant web page;
- Ensures privacy and anonymity;
- Provides a secure payment system;

---

<sup>5</sup>We will discuss 'Threats to Internet Payment' in Section 5.1 on page 54.

- 
- Provides payment cancellation facility;
  - Small amount of time for payment transaction;
  - Supports the issues <sup>6</sup> of a secure Internet payment systems;
  - Unchanged shopping habit for customer.

However, there are still some deficits in our model.

- Our model is primarily designed for the ease of merchant. Therefore, no a definite interface is developed for the customer's requests.
- Our model is not universally compatible with other Internet payment systems, so that the merchant is difficult to utilize several payment methods at a time. In order to do that, the merchant has to incorporate different payment systems into the web server.
- Assume the merchant is bad and wants to earn a profit from the online shop, he will surely tell lies to his customers and no outstanding orders will be handled. Customers' credit card will be debited and no services will be provided.

According to the third deficit described above, we have an assumption throughout the research project. We assume all merchants are honest guys so that order cancellation is available and possible if necessary.

The cancellation feature of our system is composed of two parts: order cancellation and payment refund. The merchant web server will handle the order cancellation, while our payment system will handle the payment refund. Only the purchased customer can cancel the order successfully. If the cancellation service is triggered, the order will be cancelled if all the following prerequisites are satisfied:

- Customers have ordered product(s) from the merchant online shop successfully.

---

<sup>6</sup>We will discuss 'Aspects of A Secure Internet Payment System' in Section 5.2 on page 5.2.

- The purchased product(s) has/have not been shipped out from the merchant shop.
- Customer can provide the order reference ID to the merchant for authentication of the correct customer.

For the payment refund, the customer has to provide their credit card detail, which is used for that order request, together with merchant acknowledgment send to our payment system. After authentication and verification of the credit card detail and the order payment, the customer's credit card account will be refunded if the transaction has already been done.

## 2.3 Model Architecture

In this section, we talk about the architecture of our model. We first discuss the message contents of our model and its payment flows, and hence we discuss the system flow of our model in the payment process.

We now introduce the notations used in describing the message content. Table 2.1 lists out all the notations used.

The mechanism of our payment model is shown in Figure 2.2. The payment process is described in four steps, and the details of the information flows are as follows:

- i The customer first goes to the merchant's web page and browses products, and puts the selected goods into a virtual basket. After the customer finishes choosing the products, the payment process is triggered by clicking a button. A secure connection between the customer and the merchant is established using SSL protocol for communications. The customer then enters personal information and credit card information into the browser. In addition, the product information and the total amount will be included in the message which is sent to the merchant. The message content ( MC1 ) in this step is



Name	Description
address	The mailing address of the customer.
amt	The total amount of the purchased goods.
card_name	The name of the credit card holder.
card_no	The credit card number of the customer.
card_type	There are three types of credit card: MasterCard (MC), VISA (VS), and American Express (AE).
e_date	The expiry date of the customer's credit card.
p_opt	There are two payment options: using credit card (CC), and using electronic coins (EC).
prod_id	An identification number for different products.
quan	The total quantity of the purchased goods.
receipt	An unique number recording the transaction for future retrieval when needed.
RESULT	An acknowledgment from acquirer to merchant, and also from merchant to customer, stating whether the transaction is completed or aborted.
SIG	The digital signature of a message. It uses the sender's private key to sign on message digest.
X_cert	A public-key certificate of different parties, denoted by X. It is composed of the acquirer's name, the public-key, and trusted third party's name. X = Payment Gateway (pg) or bank (bank).
X_id	An 8-digit unique number for different parties X. X = bank (bank) or merchant (m).
X_name	The name of party X. X = customer (cust), or merchant (m).
X_priv	The private key of party X. X = PG (pg), bank (bank), customer (cust), or merchant (merc).
X_pub	The public key of party X. X = PG (pg), bank (bank), customer (cust), or merchant (merc).

**Table 2.1:** Notations Used in the Message Content of Payment System

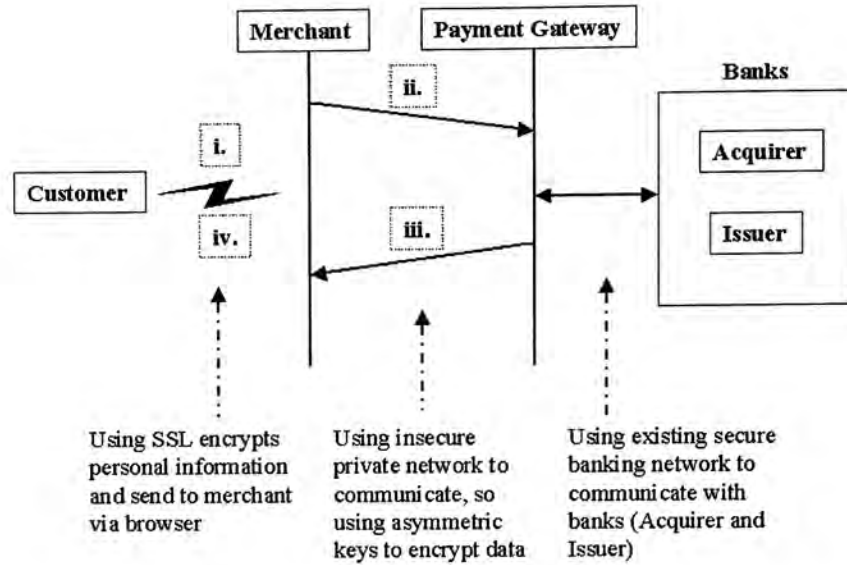


Figure 2.2: Our Payment Model and Its Payment Process Flows

MC1:

$\{card\_name, card\_no, e\_date, card\_type, address, prod\_id, quan, amt, p\_opt\}_{bySSL}$

- ii Upon the receipt of message MC1, the merchant can get the personal information and credit card information of the customer. The merchant then requests payment authorization and validation of credit card from cardholder's financial institution by composing a message ( MC2 ) which consists of the customer's personal and credit card information, together with the total amount and the merchant's name. This message will be encrypted by the merchant's private key to serve as an authentication. A header, which contains the merchant identification number and a number, denoting the payment option the customer chose, is attached to the message. The whole message is encrypted with the payment gateway's public key to prevent eavesdropping and message tampering. At this step, the merchant will send out the message packet to the PG as

MC2:

$\{\{card\_name, card\_no, e\_date, card\_type, amt, m\_name\}_{merc\_priv}, m\_id, SIG, p\_opt\}_{pg\_pub}$

- iii When the PG receives the message ( MC2 ) from the merchant, the PG first uses the private key to decrypt the message to get a decrypted message and a header. The PG will notice the message is sent by a specific merchant but only the merchant's public key can decrypt the header message. Next, PG will communicate with the issuer ( the bank issue customer's credit card ) and the acquirer ( the bank where merchant's account resides ) through an existing banking network which is assumed secure. After the PG receives the response from the issuer and the acquirer, the PG will compose a message ( MC3 ) including the response ( whether the credit card is valid and the purchase is within the credit limit ) and a receipt to the merchant for record purposes. It is then encrypted by the PG's private key for authentication. In addition to the message, the PG's certificate is adhered to the message. The whole message is encrypted by the merchant's public key for privacy and security purpose.

**MC3:**

$$\{\{RESULT, receipt, m\_name\}_{pg\_priv}, SIG, pg\_cert\}_{merc\_pub}$$

- iv Upon the receipt of the PG's message, the merchant will decrypt the message using the private key and then using PG's public key to obtain the original message. After checking the result, the merchant will compose a message ( MC4 ) to inform the customer if the purchase is successful or not. The message will be displayed as an html document for the customer. The message can be decrypted by the SSL for the privacy purpose.

**MC4:**

$$\{RESULT, receipt, prod\_id, quan, card\_name, address\}_{bySSL}$$

After this confirmation message is sent to customer, the payment process is said to be complete.

Figure 2.3 illustrates the system diagram of our model. Our system accepts three requests: payment initialization, payment capture, and payment cancellation. The merchant and the customer initiate the requests. The customer has to submit his



credit card details ( i.e., his name on the credit card, his credit card number, expiry date of his card, and the brand of his credit card. ) together with the merchant details ( i.e., name, identification number, banking account number, and transaction amount. ) to our system server to handle the payment initialization request. After our system received the response from the bank, we will send the acknowledgment to the customer to notify whether the transaction was authorized.

Another case of requesting payment capture is similar to the payment initialization. Every evening, the merchant web server will ask for payment capture process by sending a batch of transaction records which the payments are not yet captured. Our system helps the merchant to communicate with the bank to capture the funds. The merchant web server will receive an acknowledgment after our system received the acknowledgment from the bank system.

For the request of payment cancellation, our system will communicate with the bank systems and the merchant server in order to check against every transaction details. If all parties authorize the payment cancellation request, then the transaction is aborted and the bank will not debit the customer's credit card account or credit the merchant's banking account. The payment can be cancelled if and only if the payment is not captured yet. In addition, the following information has to be supplied for canceling the payment order:

- provides the credit card details corresponding to the payment order ( from customer );
- provides the payment ID, a unique number to identify which payment order of the transaction ( from merchant );
- provides the reference ID, a unique number to identify which payment order of the transaction ( from customer );
- provides the time of payment authorization of the payment order ( from merchant ); and
- provides the name and the URL of the online shop ( from customer ).

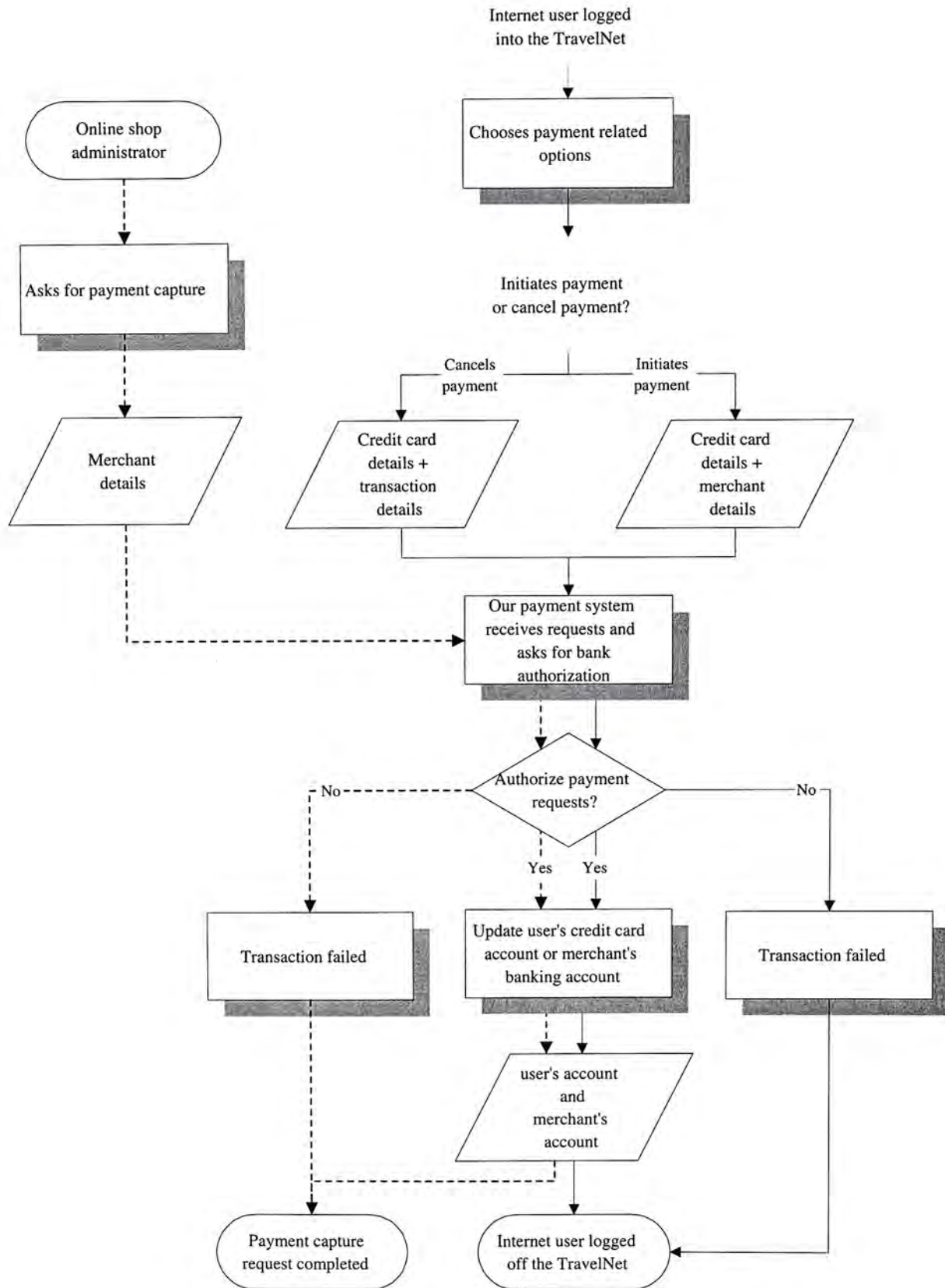


Figure 2.3: System Flow Diagram of Our Payment Model

	<b>Payment Options</b>	<b>Cryptography level</b>	<b>Anonymous</b>
Our model	credit card	intermediate	yes
CyberCash	credit card & e-cash	high	no
QIPP	credit card	intermediate	yes
SET	credit card	high	yes

**Table 2.2:** A Comparison between Our Payment Model and Different Internet Payment Systems

## 2.4 Comparison

Table 2.2 is a comparison between our payment model, CyberCash, QIPP and SET.

We compare our model with other payment systems in the area of payment options provided, cryptography level achieved, and anonymity provided. Our system will not record the customer's transaction details; therefore, anonymity is preserved. For the payment option, although we only accept credit card now, we provide a payment option field in the message packet for future addition of electronic coin payment. The level of cryptography is in intermediate level. By comparing cryptographic techniques in other payment systems with our model, we state our level is intermediate because we did not put too many cryptographic algorithms inside our model. However, our model is secure to handle the online payments. The discussion on the security of our model is found in Section 5.3.

## 2.5 System Implementation

We implement our payment model by using Java <sup>7</sup> [17] programming language ( Java Development Kit version 1.2.2 ). To be efficient in implementing our system, an additional Java package called logi.crypto [21] is served as a tool for developing the encryption and authentication in our payment model. Logi.crypto is a non-certified

<sup>7</sup>Java is a Trademark of Sun Microsystems.

100 percent pure java library for using strong encryption in your java programs. The customer's credit card account and the merchant's banking account are stored in an Oracle 8i [31] database. Verifying the customer's credit card account is the same action as retrieving the data from the database for checking. Debiting or crediting an account is the same action as updating the corresponding records in the database.

The whole system includes an application server of our system to receive the requests initiated by the merchant, and a database to store the banking accounts of the customers and the merchants. The application server consists of five interfaces.

- Acquirer interface
- Issuer interface
- Merchant interface
- Payment Gateway interface
- Payment Cancellation interface

Besides, the database has several tables to store the customer's credit card information, the merchant's banking account information and the transaction details. The payment authorization and the payment capture are handled at different time instant in our implementation, however, the time difference is within a usual frame of time period.

### 2.5.1 Acquirer Interface

It is used to handle the requests for payment capture by crediting the corresponding merchant's banking account. It will verify whether the merchant's account corresponds to the right merchant. If it is authenticated, it will credit merchant's account and sends acknowledgment to the merchant via payment gateway; otherwise, negative acknowledgment is sent instead.



---

All activities are recorded in a log file called “acquirer.log”. It records the time and the transactions that are committed. In our implementation, the database is being called by this interface for crediting the merchant’s banking account.

### **2.5.2 Issuer Interface**

It is used to receive the requests for payment authorization, complete the requests, and send back the result whether it authorizes the payment. It will verify whether the customer’s credit card account is correct and the credit limit is not over. If both are correct, it will send back the acknowledgment to the merchant via payment gateway; otherwise, negative acknowledgment is sent instead. In addition, a reference number is given to the successful authorization and the acknowledgment contains this number for future referencing. Another aim of this interface is to debiting the customer’s credit card account in the payment capture process.

All activities are recorded in a log file called “issuer.log”. It records the time and the transactions that are committed. In our implementation, the database is being called by this interface for validating the credit card and debiting the customer’s account.

### **2.5.3 Merchant Interface**

This interface provides calls from the merchant to the payment gateway for asking payment authorization of the customer’s credit card account from the Issuer and payment capture from the Acquirer. After the customer initiated a payment request and sent his credit card information to the merchant over the network, the merchant initiate a call to sent the credit card information together with the merchant’s information to the payment gateway. The merchant will receive a response when the payment gateway received the authorization response from the Issuer and Acquirer.

When this class is initiated, it first makes a connection to the Payment Gateway with a specified Internet address and port number by socket programming. The network is secured by the use of the key encryption algorithm. After the connection is



established, they can communicate with each other securely to complete the payment order. This interface makes use of the public-key encryption and decryption to ensure the authenticity of both parties and confidentiality of the message.

#### 2.5.4 Payment Gateway Interface

It is the main system interface to communicate with the merchant, the Acquirer and the Issuer. There is a call named as 'Authorization' to responding the asking for payment authorization from the merchant. It communicates with the Issuer to validate the credit card information and authorize the payment. Another call named as 'Capture' is for capturing and settling of payment transactions from the Issuer and Acquirer. The interface will pick out the relevant information to accomplish the payment authorization or the payment capture and forwards them to the Issuer or Acquirer respectively.

This class is implemented by Java Thread programming. Therefore, it allows multiple merchants to communicate with the Payment Gateway concurrently. Besides, all activities are recorded in a log file called "pgate.log". When there was system down, the transaction can be recovered from the file.

Moreover, the payment gateway ( PGate ) class has to be non-stop operating to handle the requests from Merchant class and responses from Acquirer class and Issuer class.

#### 2.5.5 Payment Cancellation Interface

This interface is for the canceling of payment by the customer. Whenever the customer initiates the payment cancellation function, he has to authenticate himself by providing the reference number of the particular payment, his credit card information, the time of the transaction, the name and the URL <sup>8</sup> of the online shop. In this state, the customer can only cancel the payment successfully if and only if the payment is not

---

<sup>8</sup>URL is the short form of Uniform Resources Locator.

yet committed. However, this interface is only initiated by the merchant, but not yet implemented by the customer initiates.

## Chapter 3

# A E-Commerce Application – TravelNet

To demonstrate our payment model in a realistic environment, we integrate it into an e-commerce application called TravelNet<sup>9</sup> [37]. TravelNet is a project that simulates a real life E-commerce application, i.e., an online traveling agency. There are similar e-commerce applications in the web, for example, Expedia [12] and Travelocity [38]. TravelNet is a Web application [40] and it provides services like flight reservation, travel accessories selling, tour guides, and hotel reservation. Secured credit card payment [35] will be done by our payment system mentioned in Chapter 2.

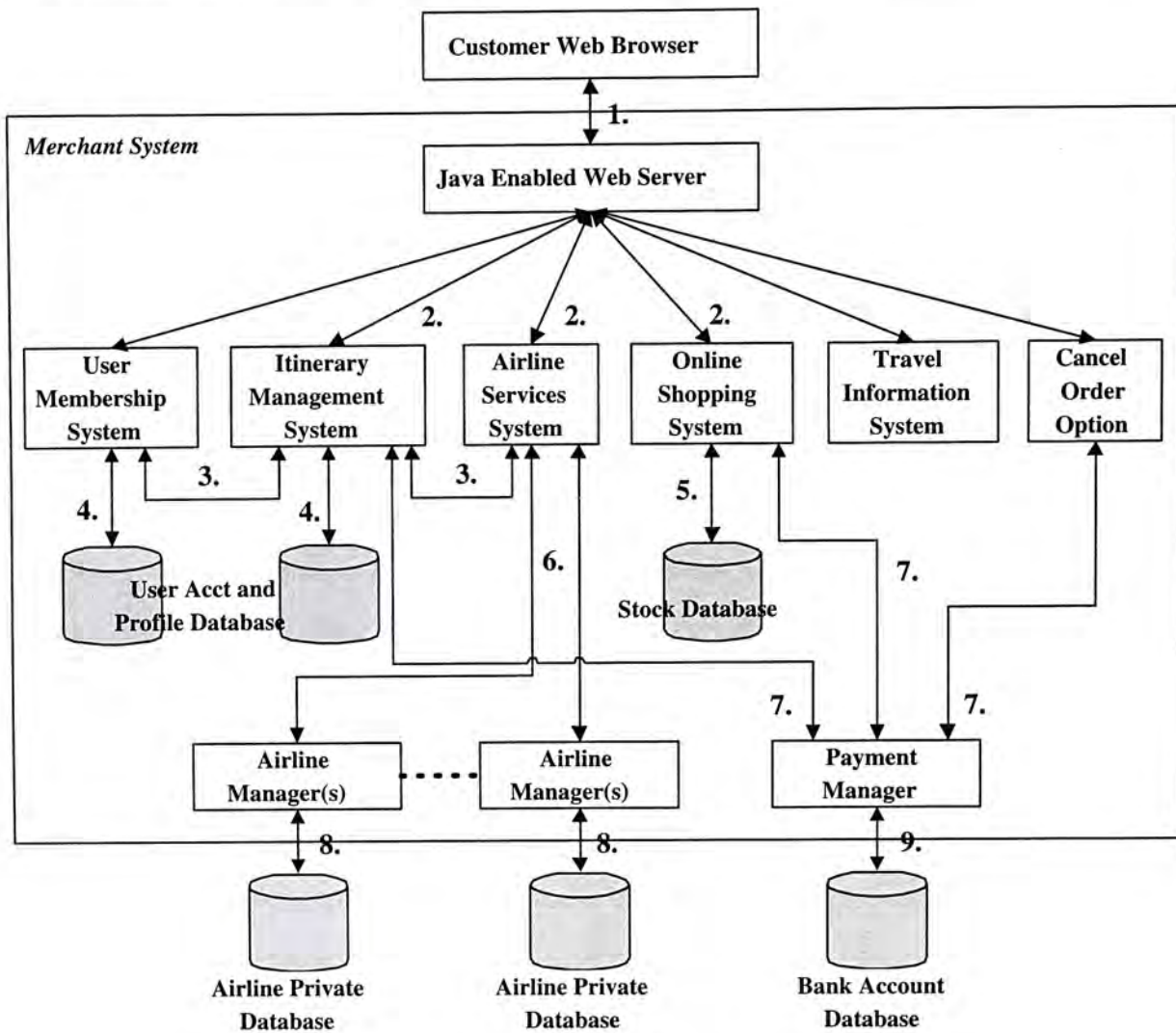
The followings briefly describe the architecture, features, and appearance of TravelNet, and how it cooperates with the payment system through a Payment Gateway ( PG ).

### 3.1 System Architecture

The overall architecture of TravelNet is shown in Figure 3.1. Details of the information flow are described as follows:

---

<sup>9</sup>Arthur C. H. Lau and Malcolm C. H. Ho, who were final year undergraduate students in year 1999/2000, built TravelNet excluding the Payment Manager.



**Figure 3.1:** Overall Architecture of TravelNet

- 1 The customer web browsers will retrieve information and generate requests to the web server, which TravelNet is hosted on by means of standard HTTP protocol. In normal situation, the information transmitted between is not confidential data that the data will not be encrypted. This can ensure a faster response. However, in some occasion that user's private information, like password and credit card number, are transmitted, SSL connection are provided that it can lower the risk of data being captured and interpreted by third parties.
- 2 Web server that is Java enabled will direct request and call the appropriate components of TravelNet to provide services. Requests can be divided into two

types: a) requests for static pages like travel guides, and b) requests for dynamic service, which involves servlet [9, 40] invocation.

- 3 There is the possibility that one particular service is done together by the co-operation of different components in the system. For example, itinerary list is updated once the reservation of flight succeeds. There should be a communication channel between these components for such cooperation to exist. In Java, calling corresponding object's method, which is a general strategy of message passing in object oriented programming environment, can easily do this.
- 4 There is a database to store the user account information, which includes the user profile and their itinerary list. Since they are local to the system, all access to these databases is done by direct connection using Java Database Connectivity (JDBC).
- 5 Again, for the online travel accessories shop, it has a stock database to keep track of the stock information. It is similar to the situation of user account database that they are local to the system and can be accessed directly using JDBC.
- 6 Flight related operations are needed for booking flight and queries. Since TravelNet should not have right for direct access to the databases of each airline. Therefore, all the operations are provided abstractly by Airline Manager, which serves as a dealer to the particular airline. These Airline Managers should be act as a coded client provided by each airline to support such operations.
- 7 Payment request will be generated during transactions. Similar to the case of flight operations, all banking operations are done through the Payment Manager via the Bank Interface.
- 8 This is the internal access between the Airline Manager and the own set of databases. It is outside of TravelNet system.
- 9 This is the internal access between the Payment Manager and the own set of bank databases, It is outside of TravelNet system.



## 3.2 System Features

A number of features are provided based on the architecture of TravelNet. They include:

- **User Registration and Profile Management:** Users should register for membership before using TravelNet online reservation and shopping service. After being a member of TravelNet, the users can login the system to use the service and change their profile whenever they want.
- **Flight Search:** Users can search for available flights by means of one of three methods, i.e., the one-way search, the round-trip search and the multiple destinations search. Once they have searched for a suitable flight, they can add the item in the Itinerary for reservation of tickets.
- **Itinerary Management:** Users can view and modify their itineraries with this service. They can also confirm the reservation and trigger the payment service for the reservation.
- **Travel Accessories Shop:** Users can buy traveling accessories like luggage, maps and travel guide books in this online shop. They can add and remove items in a shopping basket during their shopping time. Finally, they can check out the shopping basket and request the payment gateway for payment.
- **Travel Guides:** Users can obtain tourist information of the cities covered by TravelNet so that it will be convenient for them to plan for their trips.
- **Order Cancellation:** Users can cancel the order successfully unless their purchased products have not been shipped out and they submit the correct personal information for authentication and verification. If the order is cancelled successfully, users will be refunded.

### 3.3 System Snapshots

Figure 3.2 is the snapshot of the main page of TravelNet. In this page, users can easily select the services provided by TravelNet which include:

- 1 The member accounts where users can view and update their itineraries and account information;
- 2 Flight search and reservation where users can search flights with different search methods;
- 3 Hotel reservation which allows users to reserve hotels for their trip;
- 4 Online travel accessories shop which users can buy travel-related accessories;
- 5 Travel guide which provides a basic reference for users to plan for their trip.

Figure 3.3 is the snapshot for a round-trip search in TravelNet. In this page, users should provide the system with some information about their trips for the system to get related flight information from the foreign inventory databases. The information required are grouped as four parts:

- 1 *When and where is the trip:* Users should inform the system about the departure place and the target place, and the date and time of departure and return of the trip.
- 2 *Who is going on the trip:* Users can choose the age group of the target ticket holders for the best price.
- 3 *Flight preferences:* Users can choose the class of service among the first class seats, business class seats and economy class seats. They can specify the airline they want to take and also some price-reduction-related options.
- 4 *Start the search:* Users can select whether the search result should be sorted according to the best deals, or a complete list should be displayed.

**LYU9901:  
TravelNet**

Home Page

**Ad. Banner Here**

**Member Flight Hotel Shopping Guide**






## Welcome to TravelNet

This is an online travel agent to help you to reserve airline tickets for the flights between six major Asian cities and the respective hotels. We also provide a shopping service for travelling accessories at your convenience.

If you are our new visitor, please have a [free register](#) 1st!


**WEB SPECIAL**

**Customer Support**  
[Join now for free](#)  
[Payment in credit cards](#)  
[General information](#)

-  [View and update your current itineraries and account information](#)
-  [Search air-fares between cities and reserve the air tickets](#)
-  [Describe of the hotels in the cities and reserve for rooms](#)
-  [Get the necessary travelling accessories in our online shopping centre](#)
-  [Detail introduction to the cities to help you design a comfortable tour](#)

Home Page

**Member Flight Hotel Shopping Guide**

  
powered by CUHK

The project is developed and maintained by FYP group LYU9901,  
**Computer Science and Engineering Department,**  
**The Chinese University of Hong Kong.**

All materials in the homepage are copyrighted to their holder and should be here for educational purpose only. Please [email](#) to us if the materials here offend your copyrights. We will remove it as soon as possible.

**Figure 3.2:** Main Page of TravelNet

Figure 3.4 shows the shopping basket check-out screen when users are shopping for travel accessories.

- i Selected items in user's shopping basket. The shopping basket will be kept along with the logged-in user and store the items the user is interested in. The items in the basket can be added or dropped at the user's discretion.
- ii Total amount of all the items in the user's shopping basket will be calculated and displayed as a reference before the user checks out.
- iii Check-Out information should be typed in this box. This information will be sent to payment system securely ( via SSL and public-private key technique ) for

authentication and payment validation.

iv Click this button will start the payment transaction.


After the transaction is done, the screen will be displayed as shown in Figure 3.5 as a confirmation. The total amount deducted and where the amount is deducted from will be shown. Additionally, a reference number is provided for the user to check for his/her payment record in the future.

After the transaction is complete, the user can logout current session or continues using the services provided by TravelNet.



Home Page

[Member](#) [Flight](#) [Hotel](#) [Shopping](#) [Guide](#)



**WEB SPECIAL**

**Search Option**  
[One Way](#)  
[Round Trip](#)  
[Multiple Destination](#)

**Round Trip Search**

**1. Where and when do you want to travel?**

---

Select the city from the list

From:

To:

Departing: (Month-Day-Year)  
 -  -

Departure Time:

---

Return Date:  
 -  -

Return Time:

**2. Who is going on the trip?**

---

Please choose the appropriate age group for the ticket holder

**3. Do you have any preferences?**

---

Class:

Type: (leave it UNCHECKED for lower price ticket if it is not necessary)  
 No change penalties after purchase.

Airline:

**4. Start the search?**

---

Search the result to show:  
 Lowest price tickets  
 All possible choices

Figure 3.3: Flight Search Screen



## Here is Your Basket

Dear Malcolm Scud, **Shop Again**

Drop ID	Product	Category	Feature	Quantity	Price	i. Selected Items
Γ misc1	misc			2	4.5	ii. Total Amount
Γ oyster1	luggage	Criton		1	72.99	
Total (US\$):					81.99	

**Update Basket**

iii. Credit Card Information to Request Payment

Name of Cardholder: Malcolm Scud Credit Card Number: 1111222233334444 Credit Card Expire-Date: 07/2000	iv. Checkout by the Card Information <div style="text-align: center; border: 1px solid black; padding: 5px; width: fit-content; margin: 0 auto;"><b>Check Out</b></div>
---	--

Figure 3.4: Check-Out Screen

**Payment Transaction Successful!**  
**Thanks for Your purchase!**

**Payment:      \$US 81.99**  
**Visa Card: 1111222233334444**  
**Reference#: 00000023**

**Shop Again**
**Logout**

Payment Compliant: [payment@travelnet.cuhk.edu.hk](mailto:payment@travelnet.cuhk.edu.hk)

Figure 3.5: Transaction Completion Screen

## Chapter 4

# Simulation

In this chapter, we present the simulation of existing payment systems. We discuss the simulated behaviors of customers and the flow of the simulation. Then we list all assumptions used throughout the simulation and describe the simulation of the payment systems: Secure Electronic Transaction (SET ), CyberCash, and Qudro-way Internet Payment Protocol ( QIPP ).

### 4.1 Objective

The objective of simulation is to build a computer model to imitate a true model and to evaluate the computer model numerically. Data are gathered in order to estimate the desired true characteristics of the model [20]. Time is saved in the simulation because the true model is simulated, but not the real complicated model to be implemented.

A system is the process of interest in the simulation. In order to study it scientifically, we often have to make a set of assumptions about how it works. These assumptions, which usually take the form of mathematical or logical relationships, constitute a model that is used to try to gain some understanding of how the corresponding system behaves.

A system is defined to be a collection of entities, e.g., people or machines that act and interact together towards the accomplishment of some logical end [34]. In our

simulation system, the entities are customer, merchant, payment system and bank. The logical end is how the payment system entity interacts with different number of customer entities and the time used when different number of payments handled at the same time.

We build a simulation model to imitate the process of the real payment systems, i.e., SET, CyberCash, and QIPP, instead of implementing them. We compare the simulation results of these systems with our system. Although the simulation results may be different from the real statistics, the results are still useful due to lack of real statistics.

## 4.2 Simulation Flow

We build the simulation model using Java programming language ( Java Development Kit version 1.2.2 ). In addition, we include a Java package library called JavaSim [18], a set of Java packages for building discrete event process-based simulation.

The emphasis on our simulation is in the purchase request stage in the payment system. The stages of a simulated online transaction are similar as we discussed in Section 2.1 on page 19. The flow of an online transaction simulation is shown in Figure 4.1. The stages are as follows:

- 1 Customers are generated randomly who browse through the online shop in a random period of time;
- 2 Customer, who purchases online, will initiate the payment request;
- 3 Merchant asks banks for the payment authorization and the payment capture via the payment system;
- 4 Requests will be completed in a random period of time; then acknowledgment will be sent back to the merchant; and
- 5 Acknowledgment will be sent to the customer.

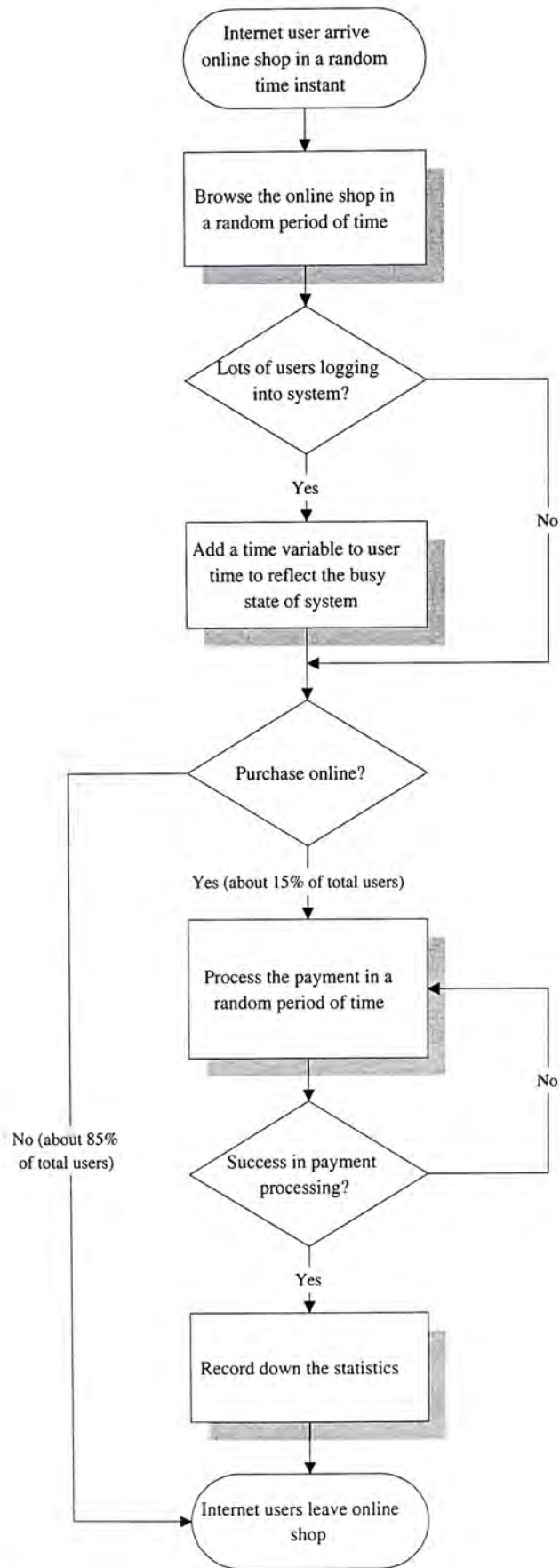


Figure 4.1: Flow Diagram of the Simulation

After the simulation finished, the statistics are being recorded in a file. The statistics include the average customers browsed the online shop, how many transactions are done, how long for a transaction to be completed, and the time differences between a transaction completed in a high time and a transaction completed in a low time.

The configuration details of the simulation run can be found in the Appendix B. In Figure 4.2, we illustrate the simulation model architecture, different entities, and the interaction between them. The descriptions are as follows:

- There are two final states in the simulation model: 'Payment finished state' and 'No purchasing state'.
- The arrival rate of Internet users is exponentially distributed.
- The Internet users browse the online shop for a period of time, which is uniformly distributed.
- After a certain period of time, the Internet users finished browsing the online shop. If they found some favorite goods and liked to purchase them online, they will move to 'Purchasing state'; otherwise, they will move to the 'No purchasing state'.
- There is a chance of  $\alpha$  percent, the Internet user will purchase online ( i.e., move to the 'Purchasing state' ).
- There is a chance of  $1 - \alpha$  percent, the Internet user will not purchase online ( i.e., move to the 'No purchasing state' ).
- Inside the 'Purchasing state', there are different number of stages ( states ) to complete a transaction. The number of stages ( states ) depends on which payment systems ( i.e., SET, CyberCash or QIPP ) is simulating.
- All the stages inside the 'Purchasing state' are followed under the real system stages in processing payment.
- Those stages are using time variable from a statistical distribution to randomly determine the simulated time.



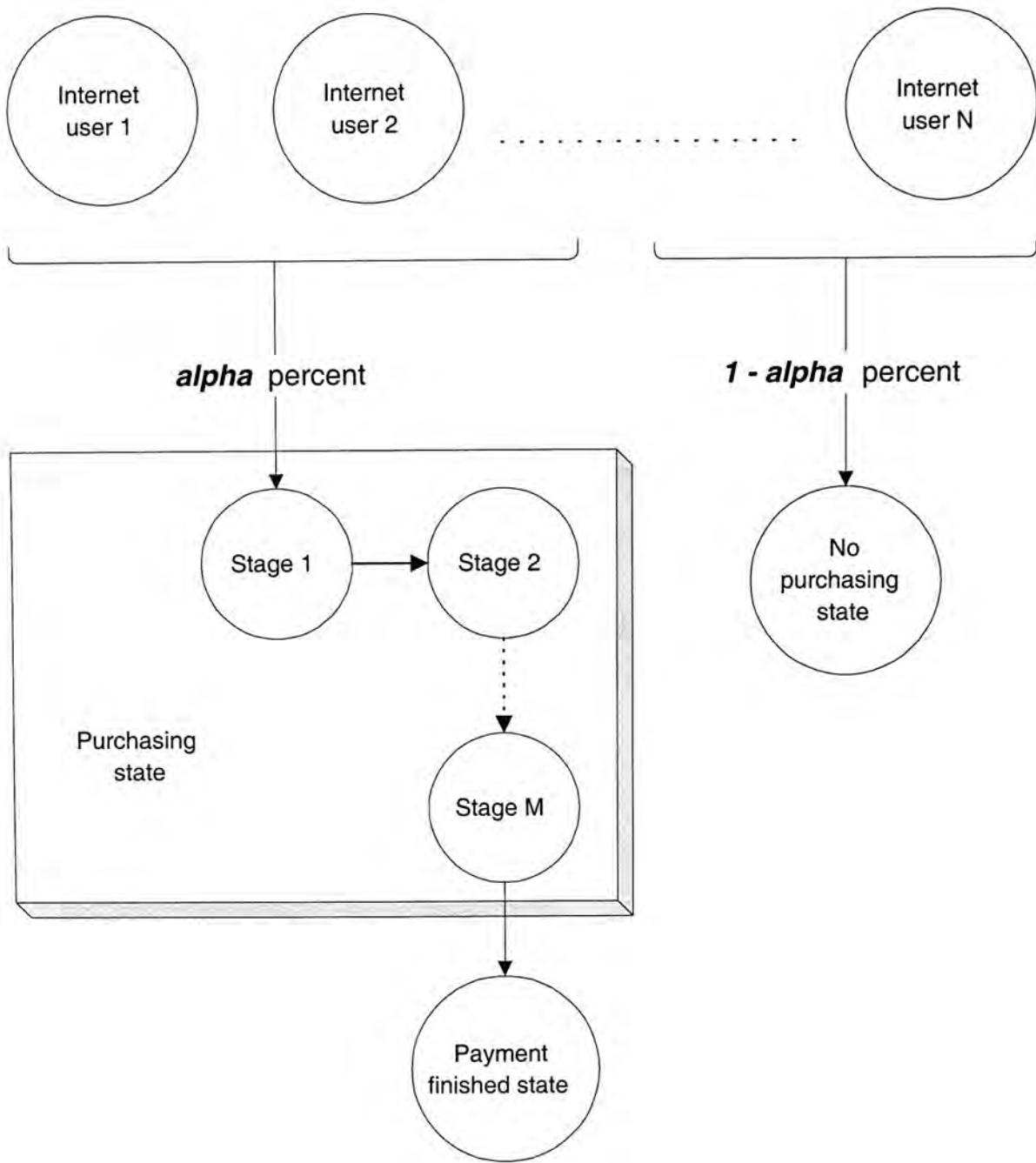


Figure 4.2: Interaction between Different Entities in the Simulation Model

- For each stage in the 'Purchasing state', the time used to move from one stage ( state ) to another stage ( state ) is randomly generated. It depends on the message content of each stage ( state ) to complete.
- After the state moves to 'Payment finished state', the transaction is said to be complete.

### 4.3 Assumptions

Here we list out all assumptions on the simulation of different payment systems:

- All time variables are in the unit of seconds.
- All time variables are with mean  $\mu$  seconds and standard deviation  $\sigma$  seconds generated from distribution functions ( Exponential, Uniform, Normal, Poisson, etc. ).
- The time of requesting the web page and responding the customer are included in the roaming time variable.
- Each customer has two behaviors only. Either they will pay for the goods at most once ( one payment is processing per customer ) or they will roam around another web page without buying goods.
- No time is counted into the initializing of wallet software in the customer side.
- The payment processing time will be counted by a combination of time variables ( encryption, decryption, database connection, database retrieving and message composing ).
- Different payment systems have a bit different implementation in the area of payment processing. However, there will be no changes on the behavior of the customer.

- For each customer, he/she has two states in the simulation run, either he/she roams around the web page or pays the goods in the web page. In simple words, there are two routes for the customer to behave in the web page. One route is from roaming  $\rightarrow$  paying  $\rightarrow$  leaving the web page; the other route is from roaming  $\rightarrow$  leaving the web page.
- The customer arrival time ( when he/she requests the web page ) variable and the roaming time ( total time used in the web page other than paying goods ) variable are randomly generated using an exponential distribution.
- All the parameter settings, the mean and standard deviation of statistical distributions can be found in Appendix B.
- Internet user can request the online shop in any random period of time. No time-dependent behavior in our simulation.

## 4.4 Simulation of Payment Systems

We simulate the SET payment system and compare with our payment model. We will simulate the purchase request, the payment authorization and the payment capture processes only. The cardholder registration and the merchant registration processes are assumed to take place before the customer initiates the payment transaction to the merchant.

The simulation run will follow the procedures as shown below:

- 1 The simulation is used to mimic a real environment which the payment system handles the online transactions.
- 2 We use a time variable to simulate the arrival times of incoming customers. They are exponentially distributed.
- 3 We also use a time variable to simulate the browsing time of customers. That is the time used on choosing their favorite products from merchant online shop.

- 4 The customer will initiate the payment request. The simulation model will carry out a series of operation based on the payment system we are using.
- 5 We use socket programming to simulate the real communication between merchant online shop and the payment system.
- 6 The encrypting process and decrypting process will be mostly based on the statistical distributions. All values are randomized so that it is not a deterministic simulation.

### **SET protocol**

We first simulate SET protocol. To be more realistic in our simulation, we define six payment related states for the SET. The sequence of six states is:

- 1 Initiates request;
- 2 Initiates response;
- 3 Purchase request;
- 4 Authorization request;
- 5 Authorization response; and
- 6 Purchase response.

We follow the message contents of each step from the SET protocol. The time for encryption, decryption, generating a new symmetric key, generating digital signature, and verifying message integrity are all randomly distributed. The statistical distributions for the parameters are defined in Appendix B.

### **CyberCash**

We simulate the CyberCash payment system which is only for credit card payment. Same as the SET simulation, we build a computer model which consists of six states. The sequence of six states is:

- 1 Click 'Pay';
- 2 Payment request;
- 3 Credit-card pay;
- 4 Authorization capture;
- 5 Charge action response; and
- 6 Charge card response.

The difference between CyberCash and SET is small. The major difference is that there exists a system server in the CyberCash which serves as the communicator between the banks and the merchant. Also both the merchant and the customer have to apply the service and the CyberCash account, but no need in the SET.

### **QIPP protocol**

Finally, we simulate the QIPP payment system. We build a computer model, which consists of six states which is the same as the real system. The sequence of six states is:

- 1 Send bill;
- 2 Initiate payment;
- 3 Authorization of challenge;
- 4 Challenge response;
- 5 Authorization reply; and
- 6 Send payment slip.

The objective of the QIPP protocol is to provide a new way of electronic payment system. The security level is high because the merchant will not obtain any credit



card information from the customer. Accurately speaking, customer's credit card information will not be transmitted to the merchant web server; instead, it will transmit directly to the bank system. This eliminates the threat of credit card details lost in the merchant system either by man-made mistake or computer bugs.

We carry out the simulation runs in different configurations. The simulation results will be discussed in Section 6.3.

## Chapter 5

# Discussion of Internet Payment Security

Security is a major concern in the area of Internet commerce. Security ensures that authorized parties are properly authenticated and their messages are sent through a network unaltered. It can protect the customer's information and the merchant's information from unwanted disclosure in the Internet. In addition, it also gives confidence to the Internet users to purchase online. In this chapter, we will first discuss four threats to the Internet payment and four basic aspects of a secure Internet payment have to be fulfilled. Based on the threats and aspects we discussed, we will study and evaluate our model's security. How we can solve the problems of the threats and keep the four aspects of a secure system in our model. We will compare our model's system with others. Finally, we will discuss the security of a complete E-commerce application, TravelNet, which our model was incorporated into it.

### 5.1 Threats to Internet Payment

Security is never absolute in the physical world. In the Internet environment, security is a problem that accounts for only a small number of Internet users who have purchased online. The threats to Internet payment are one of the important barriers that stymie the progress of I-commerce. As concerned by the Internet users, the threats

lower down their confidence in purchasing online using credit card or electronic cash. They are afraid of losing their personal information as well as losing money. To avoid the disclosure of their privacy to an intruder, the Internet users prefer not to purchase online. However, there are ways to protect against the threats: eavesdropping, masquerading, message tampering, and replaying.

### **5.1.1 Eavesdropping**

Eavesdropping allows a network intruder to make a complete transcript of network activity. As a result, an intruder can obtain sensitive information, such as, personal information, credit card information, passwords, and procedures for performing functions. It is possible to eavesdrop using software that monitors packets sent over the network. In most cases, it is difficult to detect that an intruder is eavesdropping.

To protect the secret information such as users' personal information and users' credit card information from unwanted disclosure, cryptographic functions can be used to prevent eavesdroppers from obtaining the plain data over insecure networks. Even an intruder eavesdrops the network, he only obtains the encrypted user's information that is not readable. Without using the correct cryptographic functions, an intruder cannot obtain the original message. Therefore, this threat can be minimized by the cryptographic functions implemented in the system.

### **5.1.2 Masquerading**

Eavesdropping can be used to trap user names, unencrypted passwords, and message packets sent over the network. After an intruder obtains those information, he can masquerades as another user in the Internet. The intruder can uses the user name and password and acts as the user to login to the system. For the worst case, an intruder will make use of the user's identity to do illegal things such as sending virus all over the world and breaking into companies' computer systems.

The primary solution is to protect the information sent over the network from

unwanted disclosure. Making use of the SSL protocol in the Web, users can login to the shopping mall with more safety that an intruder cannot steal their usernames and passwords.

### **5.1.3 Message Tampering**

Message tampering is a significant integrity threat that involves a cracker intercepting and modifying a message packet destined for another system. In many cases, packet information may not only be modified, but it may also be destroyed. This threat not only includes the lost of information, the users and the system may receive an intercepted wrong message packet. The intercepted message packet may interfere the users' decision and the system may be caused service down.

Using public-key cryptography, the message packet cannot be easily tampered by a cracker. Although a cracker can get the message packet, he cannot modify it according to the fields of the packet. Even though the cracker can modify the packet, the system will test the received packet every time. If the packet is different from the fields or the packet cannot concatenates to other packets, the system will recognize the failure of the packet checking and notifies the sender system to send it again.

### **5.1.4 Replaying**

Replaying refers to the recording and re-transmission of message packets in the network. Packet replay is a significant threat for programs that require authentication sequences, because an intruder could replay legitimate authentication sequence messages to gain access to a system. An intruder can replay the message in order to testing the system.

Message replaying is frequently undetectable, but can be prevented by using packet time-stamping and packet sequence counting. The system will check the message's time-stamp, if the packet comes to the system within a period of time, the system will accept the message; otherwise, the system will neglect the packet.

---

## **5.2 Aspects of A Secure Internet Payment System**

Secure messaging for Internet payment system processing has to feature the following attributes: authentication of parties, confidentiality, message integrity, and non-repudiation by either party. Some transactions require additional attributes; thus, generation of electronic coin requires anonymity of the receiving party.

### **5.2.1 Authentication**

Authentication is the proof of identity of the parties in an electronic transaction. In the online purchasing, when an Internet user starts to pay the transaction, in order to avoid the threat of masquerading of different parties, those parties should authenticate themselves to other parties.

By using public-key cryptography, the recipient can authenticate the sender of a message by verifying a digital signature – a message digest of the message decrypted using the sender's private key.

### **5.2.2 Confidentiality**

Confidentiality is the protection that the content and information of a transaction is kept private and secret from unauthorized third parties. The customer's credit card information has to be kept confidential from the merchant or other intruders in the payment processing. This is a key requirement to Internet payment system.

By using public-key cryptography to achieve confidentiality, a message is encrypted by the recipient's public key. Only the recipient has the proper private key to decrypt the message.



### **5.2.3 Integrity**

Integrity is the proof that the message contents have not been altered, deliberately or accidentally, during transmission. In the online purchasing, a modified message content may lead to an incorrect amount of money debited to the customer's account or credited to the merchant's account, and alters the cost of a product. This will make troubles to all parties involved.

By using public-key cryptography, a digital signature of the message provides message integrity. A message digest of the message is encrypted using the sender's private key.

### **5.2.4 Non-Repudiation**

Non-repudiation is the proof of agreement of the terms of transactions and prevention of denial of commitment. Without this issue, a customer can then deny what he bought in the past and will not pay for the product. This will affect the business of the company.

By using public-key cryptography, non-repudiation can be provided using digital signatures. However, long after the fact, a dispute can arise about whether the signature was created at the same time as the message. For this problem, a digital time-stamping service may be useful.

## **5.3 Our System Security**

To evaluate our model's security, we discuss our model security based on its architecture, parties involved in the payment processing, the network communication between our model and those communicating parties, the message contents sent to and received from them, cryptography techniques used, and the threats avoided in our model.

### **The Architecture**

Recall the Figure 2.2 on page 26, it illustrates our payment model and its payment process flows. From the figure, our system resides in between the merchant and the banking system. It acts as a third party between the merchant and the banks. Our system abstracts the detail of the bank from the merchant. From the architecture, the attack is mainly come from the network between the merchant and our system and the network between our system and the banking system.

To evaluate the level of security of our system, we first consider the network between the merchant and our system. In establishing this network, they have to authenticate to each other, hence, applying the public-key cryptography to encrypt the network by using the other's public key. Therefore, even an intruder obtains the message packet from the network, an intruder cannot decrypt the message into the original readable message without the proper private key. This ensures the confidentiality of the message packet.

Consider the network between our system and the banking system. The network is secured by the cryptographic technique because the protection of the banking system is behind the firewall. It protects against an intruder to intercept the system.

The cancel payment feature in our system may attract a cracker to hack the system in order not to paying money for the purchased goods. With adequate information provided to the system, a cracker still cannot modify the payment secretly inside the system without the information from the merchant system.

### **Cryptography Used**

Our system uses the public-key algorithm, the digital signature, and the message digest techniques. We use the RSA public-key system with a bit length of 1024 to make two pairs of private/public keys. One pair is for our system and one pair is for the merchant. It is used to handle the operations of authentication and message encryption/decryption. With the usage of the public-key system, no one can obtain the clean message packet without the proper key to decrypt it.

By making use of the digital signature, we can authenticate our system to the

merchant and vice versa. By making use of the message digest technique, we can assure other crackers do not modify our messages. Therefore, aspects of a secure Internet payment system are preserved in our system.

### **Message Contents**

Recall the Section 2.3 on page 24, the message contents are discussed in details. For each message, confidentiality and integrity are preserved by using key encryption method. Take an example, if a cracker obtains the message packet containing the payment capture request, it is time consuming for a cracker to hack the message, and hence modifies it. The integrity test in the system side will test whether the message packet has been modified.

In addition, authentication is done at the beginning of the establishment of the network communication. In this case, our system knows where the shop and who the merchant are.

### **Communicating Parties**

Our system only communicates with three parties: merchant's shop, Issuer, and Acquirer. Fewer parties involved in the communication will bring fewer threats in an open network and a small chance of being hacked. Three parties involved in an online payment is the minimum size.

### **Network Communication**

In the network communication, as discussed before, there are only two basic networks that an intruder can intercept the message packet. One is a network between our system and merchant's shop system, the other one is between our system and the banking system ( Acquirer and Issuer ). For the former network, the established socket is encrypted using the communicating party's public key and decrypted the network using its private key. Therefore, confidentiality is preserved in the message packet. No one can obtain the clean message from this network.

For the latter network, it is a private network that no one can go into it without authorization. Therefore, it is free of threats attacking.

### **Threats Avoided**

According to the first section of this chapter on discussing the threats to Internet payment, our system protects against those four threats ( eavesdropping, masquerading, message tampering, and replaying ). For the eavesdropping and message tampering threats, the use of key encryption and a test on the message integrity carried out in the system server prevents the threats. Masquerading of the merchant is yet a hard task as a cracker must steal the certificate and the information for authentication stage from the merchant. Also a time-stamp is added to every message to prevent replaying threat.

From the previous evaluation, we can say that our model is secure enough to protect the confidential information ( customer's personal and credit card information, merchant's banking account information ) against unwanted disclosure over the network.

## **5.4 TravelNet Application Security**

After we discuss the security of our system, we continue to discuss the TravelNet's security. We evaluate the security of the TravelNet together with our model. Our model acts as a payment system to handle TravelNet's online payments. We use similar criteria to discuss its security including the online payments.

### **Overall Architecture**

Recall the Figure 3.1 on page 36, it illustrates the TravelNet's architecture. From the figure, TravelNet provides many options to the customer. It resides in between the customer and our system and most of the tasks are carried in the server side. So the cracker should hack into the web server in order to modify and corrupt the TravelNet.



Any Internet users have to register in the TravelNet system in order to use the online purchasing or get information from them. In this case, SSL is established to protect the network in between them until the user logs off. It maintains the security of the TravelNet system and the customer.

### **Cryptography Used**

SSL is the primarily cryptographic technique using in TravelNet application. With the use of SSL, the username and password of a registered customer are kept secret and confidential. No one can get the information except the merchant system. Besides, SSL serves as a tool to protect the credit card information when a customer initiates an online payment request.

SSL is used to protect credit card numbers and other sensitive data transmitted between a user's browser and an Internet web server. It accounts for the reason why the online shop staff can view the credit card details. There may be a chance for some wicked staff stole the credit card information. In this case, TravelNet is developed to forward all the credit card information to the payment system immediately upon receipt of message packets. This approach eliminates the chances of losing customer's credit card information.

### **Message Contents**

Since all message contents are transmitted over a secure network, any intruders cannot tamper with it. In addition, customer information as well as the payment information is kept confidential.

### **Communicating Parties**

There are two parties that communicate with TravelNet system, customer and our payment system. Both parties has cryptographic technique to support, hence, the attacks are minimized.

### **Network Communication**



In TravelNet, SSL is applied to protect customer's personal and credit card information. SSL is applied in between the customer's browser and the merchant shop. When the customer logs into the system, SSL is used to protect confidentiality of his username and password from being obtained by an intruder. When the customer decides to purchase online, SSL is used to protect the confidentiality of his credit card information from being stolen by an intruder.

In the processing of online payment, the merchant system will make use of our system component to establish a secure socket network to communicate with our system server. The description on our system security was described in the previous section.

### **Threats Avoided**

In TravelNet system, eavesdropping, message tampering, and masquerading are avoided. By applying SSL to protect the customer's personal and credit card information, an intruder cannot obtain an original message content which contains the confidential information of customer. Even an intruder eavesdrops the network, an intruder only obtains an encrypted message. This prevents the threats of eavesdropping and message tampering.

It is difficult to masquerade the TravelNet system as the system has a server certificate. The certificate provides authentication that the TravelNet system server is a real one, not a masqueraded one.

From the evaluation on the overall application, we can say that the application itself gives a shopping place where the Internet users are safer to use their credit cards to purchase online. It gives confident to the customers. It is secure enough to protect the confidential information ( customer's personal and credit card information, merchant's banking account information ) against unwanted disclosure over the open network.

## Chapter 6

# Discussion of Performance Evaluation

### 6.1 Performance Concerns

As I discussed in Chapter 1, four criteria should be considered in an Internet payment system. The performance of a system also depends on these four criteria:

- System capacity;
- System security;
- Transaction cost; and
- Transaction time.

However, there is a tradeoff in the previous criteria. If the system security is set to a high level, the transaction cost and transaction time will dramatically increase. On the other hand, if the transaction cost is low, the system security will not be too high. This accounts for the relationship between these criteria.

In this chapter, we describe the experiments conducted previously to get the transaction time needed and the capacity of our system. We have simulation to imitate the

other payment systems ( i.e., SET, CyberCash and QIPP ). For the system security, we discussed in Chapter 5.

## 6.2 Experiments Conducted

### 6.2.1 Description

We conduct three experiments and get the following results:

- 1 Multiple-Threaded Model *versus* Single-Threaded Model;
- 2 Time spent on PG *versus* Total check-out time;
- 3 Time without cryptography *versus* Time with cryptography.

By (1), we conduct experiment on the TravelNet system. The system can be constructed to be a Multiple-Threaded Model ( i.e., allow requests run in parallel ) or a Single-Threaded Model ( i.e., requests only run in series ). We compare the differences when different models are used. By (2), we analyze the time spent on PG and the total check-out time of a transaction. We get the information of the overhead ( bottleneck ) of the system. Finally, by (3), we get the time differences on check-out time and time spent of PG of our system between no cryptography applied and with cryptography used.

The details of the experiment configuration and the experiment results can be found in Appendix A.

### 6.2.2 Analysis on the Results

In our experiments, the server always allows concurrent users to request a payment and all the requests can be executed concurrently. The merchant, however, can specify the type of execution scenario, either sequential or concurrent. For a single request, the total check-out time in TravelNet is between 1.7 seconds and 2 seconds. The time could

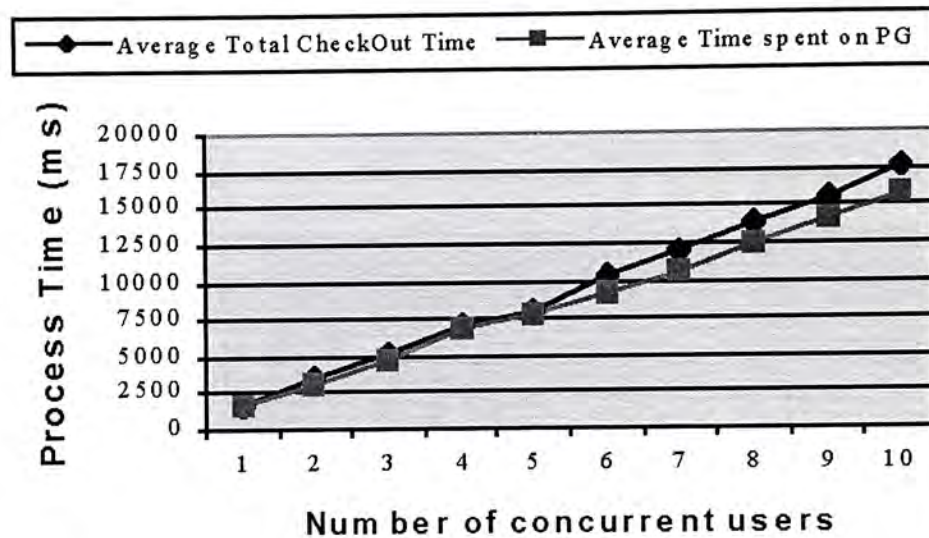
be as long as 10 seconds in the worse scenario. To filter out noises, we perform five executions to obtain the average time measure for each data point in every experiment.

From the experiment results, the time to complete a transaction was recorded as small as 1.7 seconds because the banking system does not truly reflect the real environment. We just simulate the behaviors of a banking system towards different requests, i.e., the process of asking authorization of payment, capturing payment and canceling payment contains no overhead on the network establishment between our system and banking system. Therefore, the time is a small value. To include the network overhead, our system performs a transaction in 5 - 8 seconds.

The performance measurement is based on two different models: Multiple-threaded model and single-threaded model. In the multiple-threaded model, requests are processed in parallel. Each request will obtain only a portion of the server resources, which is reversely proportional to the number of requests. For example, when there are ten concurrent users requests, each client process will be on the average ten times slower than each executing alone, as of the server resources. The time of overlapping processes will consequently be longer. There is also an extra task-switching overhead that is very significant when the number of tasks becomes large. As displayed in Figure 6.1, the payment process time increases as the number of concurrent users increases. We can also see in Figure 6.1 that the total payment process time is divided into two parts: time spent on the Merchant client, and time spent on the Payment system server. In terms of the portion of time spent for the total check-out process, payment server contributes over 80 percent.

In the single-threaded model, TravelNet clients request in a first-come-first-serve manner. Every request waits for all the previous requests to be finished before it can gain access to the server resources. Figure 6.2 shows the average total process time and the time spent on PG for the single-threaded model. As a comparison, we can see from Figure 6.3 that its average process time is much shorter than that of the multiple-threaded model. The main reason is due to database resource conflict for the multiple-threaded model when the multiple concurrent processes access the PG, which currently has only one merchant, namely, TravelNet. As the PG server resources





**Figure 6.1:** Payment Transaction Time in Multiple-Threaded Model

have to be shared among the multiple resources ( e.g., lock a data item ) and compete with each other time. In the single-threaded model, server resources are not shared among the requests and only a task-switching time is necessary between each request. As the response time is quite important in such an interactive application, the single-threaded model behaves better than the multiple-threaded model. It is noted, however, that if we have multiple merchants in the PG which handles different requests with independent merchants, the multiple-threaded model would be significantly improved.

The payment processing time can be divided into two parts as well: the time required to perform cryptography algorithms ( including message encryption and decryption ), and the time required to transmit messages and handle payments. Figure 6.4 shows the comparison on the payment process time on the PG regarding the overhead due to cryptography. We found that when the number of concurrent users increases, the gap showing the difference on the process time between using cryptographic algorithms and without using them becomes larger. This overhead indicates that for a more secure payment system, there is a tradeoff on the time to handle payment transactions. This tradeoff is quantitatively provided in TravelNet for a detailed analysis.



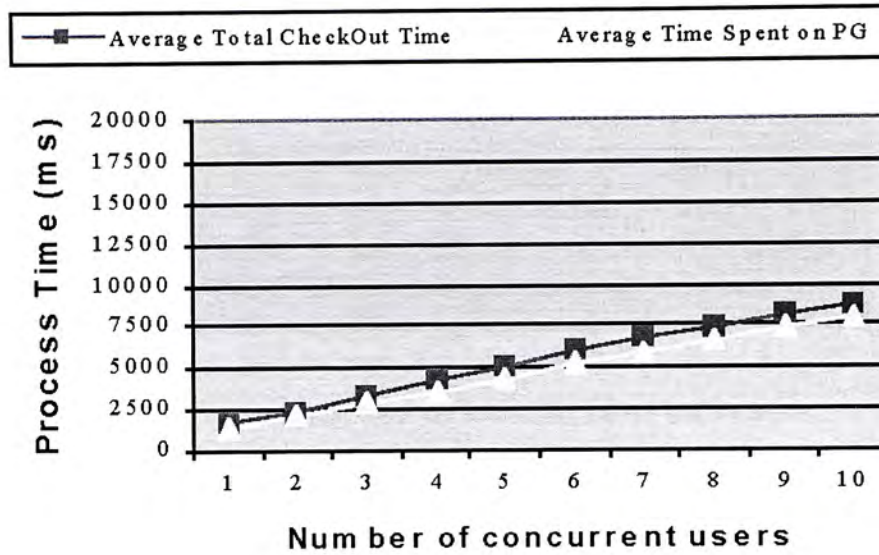


Figure 6.2: Payment Transaction Time in Single-Threaded Model

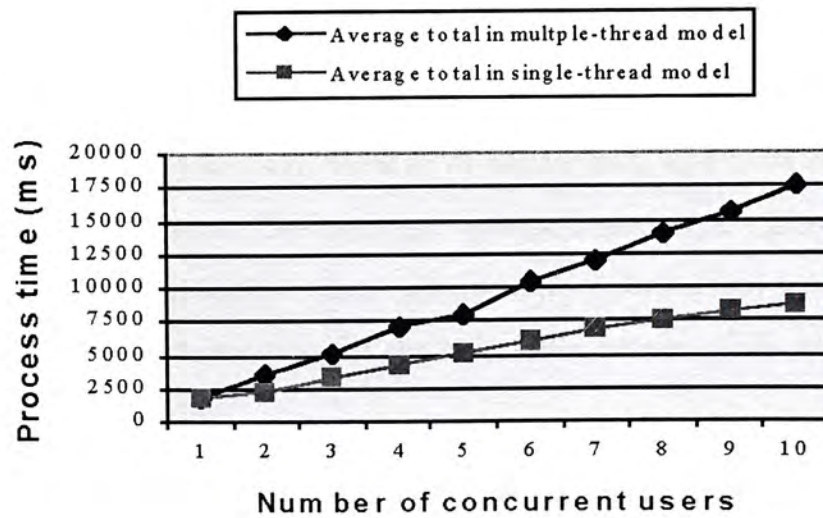


Figure 6.3: A Comparison for Single-Threaded and Multi-Threaded Model

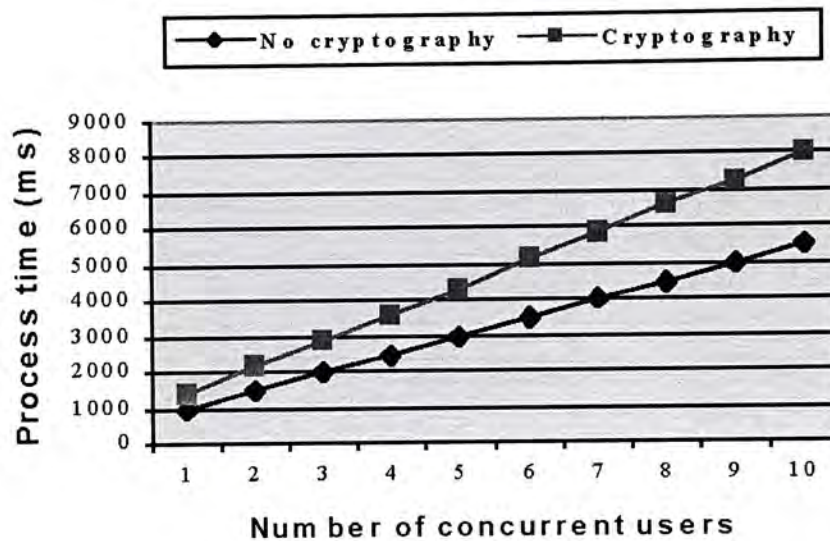


Figure 6.4: Single-Threaded Model on the Payment Transaction Time on PG

### 6.3 Simulation Analysis

The details of the simulation configuration, the parameters listing together with the mean and standard deviation, and the simulation results are depicted in Appendix B. The simulation results are based on the time consumption on the network traffic, the message cryptography, and verification of the message packet. More payment steps of the payment system will make the transaction time longer.

Figure 6.5 shows the simulation results of SET, CyberCash and QIPP. From the results, we conclude that when the number of concurrent user increases, the process time of a transaction increases. The payment transactions compete resources with each other, the network traffic is higher when there are more concurrent users connected to the payment system. These account for the increasing process time when the number of concurrent user increases.

From the comparison of the three payment systems, QIPP spent the smallest amount of time, about 28 seconds, in processing payment among these three payment systems. SET spent the largest amount of time, about 58 seconds, in processing a transaction. The time spent on CyberCash is about 52 seconds in processing a transaction.

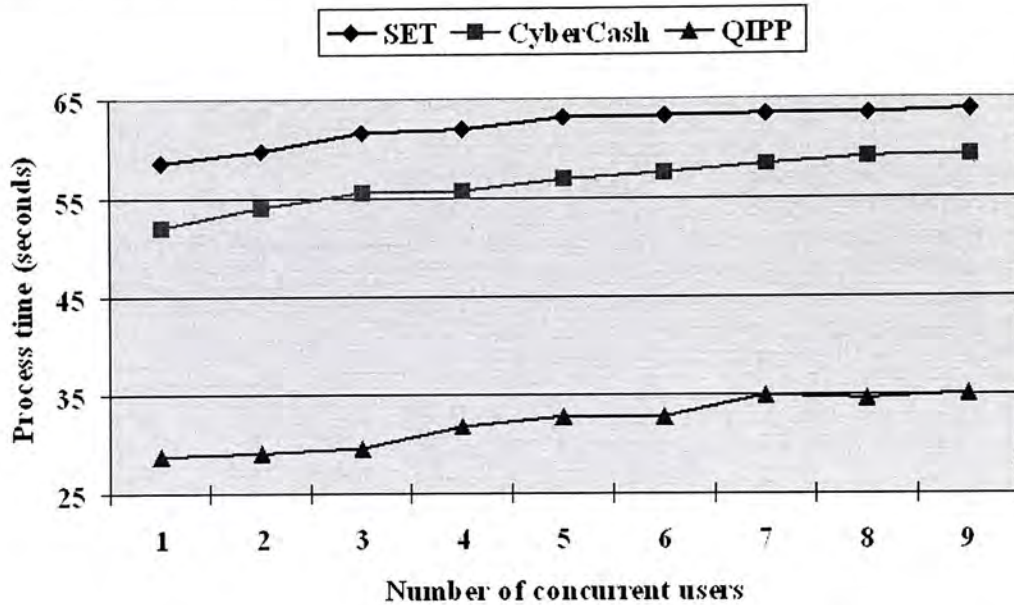


Figure 6.5: Simulation of SET, CyberCash and QIPP

In Figure 6.6, the simulation is modified on the message cryptography part. The cryptography of message encryption and digital signature are determined during simulation run. The result shows that average time used for the transaction to be completed consumes 8 to 10 seconds less than the previous simulation.

The simulation results implicated that with regards to a higher security level of a system ( i.e., longer encryption time or more encrypted messages ), the transaction time will be longer and the customer's waiting time will be longer too. On the other hand, with regards to a lower security level of a system ( i.e., shorter encryption time or fewer encrypted messages ), the transaction time will be shorter and the customer's waiting time is shorter too.



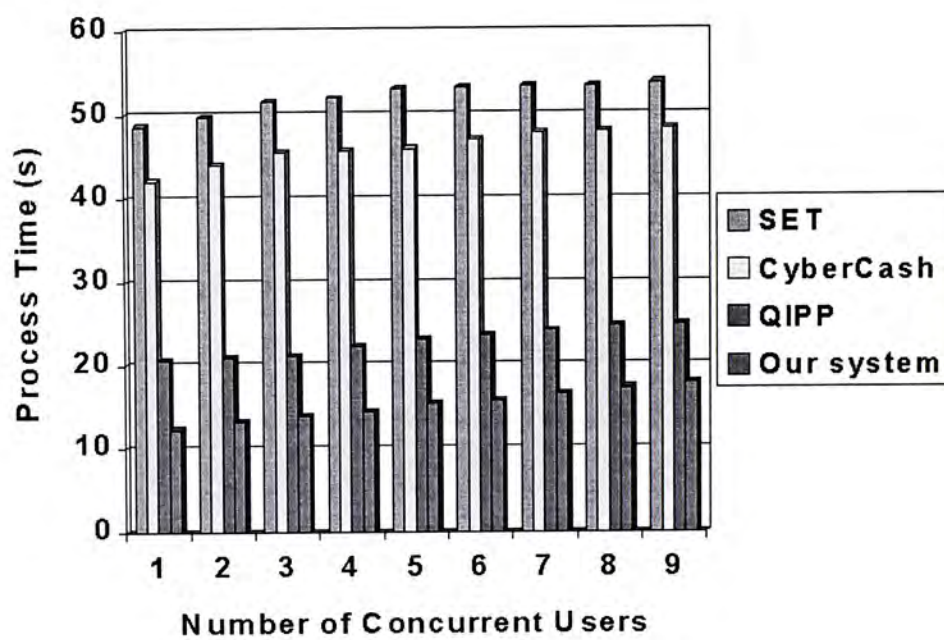


Figure 6.6: A Comparison between Our System, SET, CyberCash and QIPP

## Chapter 7

# Conclusion & Future Work

Nowadays, World Wide Web has given a new business opportunity for companies to explore. To handle the transaction in the World Wide Web, an Internet payment system serves you to do that. In this thesis report, we have discussed several existing Internet payment systems ( e.g., SET, CyberCash, QIPP, etc. ) and have compared with them to each other. They have some merits, however, also have some deficits. This account for so many payment systems have been developed and come out, not defunct yet.

We have described a light-weight payment system for E-commerce applications. Our system is easy to incorporate into a shop's web server by little modifications. Besides, the system is fast yet secure to handle the personal information from being stolen by malicious users. We have conducted experiments on testing the performance of our system as well as the E-commerce application. The results showed that our system is quick and fast enough to complete an online transaction.

TravelNet, is an online travel agent system that our payment system has been incorporated into it. The whole system mimics a real E-commerce application, delivering information as well as online purchasing. The payment system handles the part of online purchasing. Experiment results showed that the time used for TravelNet application that communicates with the payment system spent about one second.

Moreover, we have described on how the system is secure from attacks. It prevents



---

from eavesdropping, message tampering, masquerading and non-repudiation attacks. Our payment system also satisfies the aspects of an Internet payment system ( i.e., satisfies authentication, confidential, integrity and replaying ).

Furthermore, we have simulated three payment systems ( i.e., SET, CyberCash and QIPP ) to test their performance on completing payment requests. The simulation results showed that the transaction time spent in other payment systems was far longer than our proposed payment system. This concludes that our proposed payment system is fast in processing payments yet secure enough to keep data confidential in the Internet.

With regards to the data sets and the limitations in the experiments and simulations, more repeated testing on different size of data would increase the creditability of our payment model is good.

To extend the feature of our model, we can add electronic coin payment to our model. We have implemented a flag in the first message to indicate whether it is a credit card payment or an electronic coin payment. It can provide a choice for the customer to choose which one to use. Besides, our payment model can target to a market, which the value of transaction is small.

# Appendix A

## Experiment Specification

### A.1 Configuration

The configuration of the computer running the TravelNet is as follows:

- Pentium II GX1 333MHz with 96M RAM;
- Microsoft Windows NT4 ( service pack 4 );
- Microsoft IIS 4.0;
- Servlet Engine ( ServletExec 2.2 );
- Java Development Kit 1.1.8;

### A.2 Experiment Results

The experiment results are shown in Tables A.1, A.2, A.3 and A.4. The corresponding figures are shown in Figures 6.1, 6.2, 6.3 and 6.4. The numerical values of time recorded in the following tables are in the units of milliseconds. The analysis of the experiment results is discussed in Section 6.2.2 on page 65.

Number of concurrent users	Average Check-Out Time	Total	Average Time spent on PG
1	1737		1545
2	3515		3163
3	5211		4635
4	7023		6741
5	8103		7756
6	10422		9270
7	11985		10661
8	13982		12437
9	15511		14013
10	17630		15682

**Table A.1:** Experiment Result of ‘Payment Transaction Time in Multiple-Threaded Model’

Number of concurrent users	Average Check-Out Time	Total	Average Time spent on PG
1	1703		1432
2	2309		2148
3	3312		2854
4	4192		3588
5	5070		4314
6	5976		5149
7	6799		5851
8	7456		6634
9	8112		7293
10	8701		8054

**Table A.2:** Experiment Result of ‘Payment Transaction Time in Single-Threaded Model’

Number of concurrent users	Average total in multiple-thread model	Average total in single-thread model
1	1737	1703
2	3515	2309
3	5211	3312
4	7023	4192
5	8103	5070
6	10422	5976
7	11985	6799
8	13982	7456
9	15511	8112
10	17630	8701

**Table A.3:** Experiment Result of ‘A Comparison for Single-Threaded and Multi-Threaded Model’

Number of concurrent users	Average time in no cryptography	Average time in cryptography
1	998	1432
2	1501	2148
3	1975	2854
4	2480	3588
5	2982	4314
6	3485	5149
7	3984	5851
8	4475	6634
9	4978	7293
10	5471	8054

**Table A.4:** Experiment Result of ‘Single-Threaded Model on the Payment Transaction Time on PG’

# Appendix B

## Simulation Specification

### B.1 Parameter Listing

All parameters are in the unit of *seconds*. Table B.1 lists all the parameters using in the simulation, descriptions about it and the corresponding statistical distribution used.

The parameter values used in the simulation are defined in Table B.2.

### B.2 Simulation Results

The simulation results are shown in Table B.3 and Table B.4. The results are plotted in Figure 6.5 and Figure 6.6 respectively. The analysis of the experiment results is discussed in Section 6.3 on page 69.



Name	Description	Distribution
_endTime	Time length of a simulation run	—
_roam	Time for a user to browse the online shop	Uniform
_people	Number of people browsed the web page	—
_cust	Internet user arrival rate depends on the parameter <i>_people</i>	Exponential
_seed	A seed number to determine the random number generation	—
_behav_percent	The percentage of people purchasing online	—
_gen_symkey	Time for generating a new symmetric key	Uniform
_gen_dig_sig	Time for generating a digital signature	Exponential
_encrypt	Time for encrypting a message	Exponential
_decrypt	Time for decrypting a message	Exponential
_verify_cert	Time for verifying a certificate	Exponential
_verify_integrity	Time for verifying the message integrity	Exponential

Table B.1: Parameters Used in Simulation

Name	Value
_endTime	604800 ( 7 days )
_roam	( 480, 60 )
_people	50000
_cust	1.728
_seed	20000
_behav_percent	0.15
_gen_symkey	( 3, 4 )
_gen_dig_sig	1
_encrypt	2
_decrypt	1
_verify_cert	2
_verify_integrity	2

Table B.2: Parameter Values Used in the Simulation

Number of concurrent user	SET	CyberCash	QIPP
1	58.566	52.113	28.664
2	59.811	54.021	28.998
3	61.561	55.632	29.479
4	62.019	55.698	31.698
5	63.192	57.006	32.671
6	63.323	57.679	32.681
7	63.399	58.425	34.982
8	63.543	59.111	34.597
9	63.801	59.338	35.127

**Table B.3:** Result of SET, CyberCash and QIPP Simulation

Number of concurrent user	SET	CyberCash	QIPP	Our System
1	48.566	42.113	20.57	12.321
2	49.811	44.021	20.899	13.319
3	51.561	45.632	21.091	13.871
4	52.019	45.698	22.391	14.391
5	53.11	46.014	23.138	15.374
6	53.21	47.118	23.721	15.801
7	53.482	47.871	24.129	16.48
8	53.53	48.111	24.817	17.348
9	53.89	48.512	25.013	17.881

**Table B.4:** Result of Comparison between Our System, SET, CyberCash and QIPP Simulation

# Bibliography

- [1] Eastlake 3rd, D., et al. CyberCash Credit Card Protocol Version 0.8, RFC 1898, Feb. 1996.
- [2] N. R. Adam and Y. Yesha. Electronic Commerce: An Overview. In N. R. Adam and Y. Yesha, editors, *Electronic Commerce: Current Research Issues and Applications*, number 1028 in Lecture Notes in Computer Science chp. 2. Springer, Verlag, 1996.
- [3] A. Armstrong and J. Hagel. The real value of on-line communities. *Harvard Business Review*, III:134–141, May-June 1996.
- [4] Electronic Commerce Innovation Centre. An Introduction to Electronic Commerce. Technical report, Electronic Commerce Innovation Centre, <http://www.cf.ac.uk/uwcc/masts/ecic/elecomm.html>, June 1997.
- [5] D. Chaum. Blind Signatures for Untraceable Payments. In *Advances in Cryptology: Proceedings of Crypto 82*, pages 199–203. Plenum Press, 1983.
- [6] D. Chaum, A. Fiat, and M. Naor. Untraceable Electronic Cash. In S. Goldwasser, editor, *Advances in Cryptology CRYPTO' 88*, pages 319–327. Springer-Verlag, 1988.
- [7] CyberCash, Inc. <http://www.cybercash.com/>.
- [8] Product Cypher. Magic Money Digital Cash System. <ftp://ftp.csn.org>, 1994.
- [9] C. Darby. *Developing 3-Tier Database Apps w/ Java Servlets*. Java Developers Journal, <http://www.sys-con.com/java/>, Feb 1998.

- 
- [10] Editors. 50 places of a lifetime. *National Geographic Traveler Magazine*, Special 15th Anniversary Issue.
- [11] Mihir Bellare et al. iKP – A family of secure electronic payment protocols. IBM research report, T. J. Watson Research Center & Zurich Research Lab, April 1995.
- [12] Expedia.com. <http://expedia.msn.com>.
- [13] Alan O. Freier, Philip Karlton, and Paul C. Kocher. The SSL Protocol Version 3.0, Internet Draft. <http://home.netscape.com/eng/ssl3/3-SPEC.HTM>, March 1996.
- [14] Ralf Hauser, Michael Steiner, and Michael Waidner. Micro-Payments based on iKP. Dec 1995.
- [15] iamasia releases survey findings, showing 12.3 million internet users in china. <http://www.iamasia.com/presscentre/pressrel/pressrel.htm>.
- [16] S. L. Jarvenpaa and P. T. Todd. Consumer reactions to electronic shopping on the World Wide Web. *International Journal of Electronic Commerce*, 2(1):59–88, 1996-97.
- [17] The Source for Java(TM) Technology. <http://java.sun.com/>.
- [18] JavaSim Homepage. <http://javasim.ncl.ac.uk/>.
- [19] Paul Kimberley. *Electronic Data Interchange*. McGraw-Hill, Inc., 1991.
- [20] Averill M. Law and W. David Kelton. *Simulation Modeling and Analysis*. McGraw-Hill, Inc., 2nd edition, 1991.
- [21] Logi.crypto Java Package. <http://logi.org/logi.crypto/>.
- [22] MasterCard International – What is SET?  
<http://www.mastercard.com/shoponline/set/set.html>.
- [23] Gennady Medvinsky and B. Clifford Neuman. Netcash: A design for practical electronic currency on the Internet. *In Proceedings of the First ACM Conference on Computer and Communications Security*, Nov 1993.



- 
- [24] Gennady Medvinsky and B. Clifford Neuman. Electronic Currency for the Internet. *Electronic Markets*, vol 3, no 9/10:23–24, October 1993.
- [25] Millicent Microcommerce System. <http://www.millicent.digital.com/>.
- [26] Y. S. Moon and H. C. Ho. Secure Transport Protocol for E-commerce – SET versus SSL. In Wing S. Chow, editor, *Multimedia Information Systems in Practice*. Springer, 1999.
- [27] National Bureau of Standards. Federal Information Processing Standard (FIPS) Publication 46: The Data Encryption Standard, 1977.
- [28] National Institute of Standards and Technology (NIST). Federal Information Processing Standard (FIPS) Publication 46-1: Data Encryption Standard, Jan 1988.
- [29] Donal O’Mahony and Michael Peirce. Scaleable, Secure Cash Payment for WWW Resources with the PayMe Protocol Set. <http://ganges.cs.tcd.ie/mepeirce/Project/Payme/Overview.html>.
- [30] Donal O’Mahony, Michael Peirce, and Hitesh Tewari. *Electronic Payment Systems*, chapter 4.3, pages 65–67. Artech House, Inc., 1997.
- [31] Oracle 8i Database. <http://www.oracle.com/database/oracle8i/index.html>.
- [32] R. L. Rivest and A. Shamir. PayWord and MicroMint: Two simple micropayment schemes. <http://theory.lcs.mit.edu/~rivest/RivestShamir-mpay.ps>.
- [33] R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Comm. ACM*, vol 21, no 2:120–126, 1978.
- [34] J. W. Schmidt and R. E. Taylor. *Simulation and Analysis of Industrial Systems*. Homewood, Ill, 1970.
- [35] Security in Internet Transaction. <http://www.holt.ie/text/security.html>.
- [36] Marvin Sirbu and J. Douglas Tygar. An Electronic Commerce System Optimized for Network Delivered Information and Services. *In Proceedings of IEEE Comcon ’95*, March 1995.



- [37] TravelNet. <http://ntsvr4.cse.cuhk.edu.hk/>.
- [38] Travelocity. <http://www.travelocity.com>.
- [39] J. D. Tygar. Netbill: An Internet Commerce System Optimized for Network Delivered Services. 1995.
- [40] Web Application Development. <http://www.winwinsoft.com/articles/wad.html>.
- [41] J. Zhao, C. Dong, and E. Koch. Yet Another Simple Internet Electronic Payment System. *Proc. of the IFIP 1996 World Conference - Mobile Communications*, Sept 1996.



CUHK Libraries



003803719