# The Design, Implementation and Evaluation of an Internet Payment System[†]

K. L. CHONG, C. H. HO, C. H. LAU, MICHAEL R. LYU, Y. S. MOON

Department of Computer Science and Engineering, The Chinese University of Hong Kong,
Shatin, N. T., Hong Kong

{klchong, chho1, chlau1, lyu, ysmoon}@cse.cuhk.edu.hk

**Abstract**
In this paper, we propose an Internet payment system which uses a payment gateway 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 an real-life E-commerce application. On-line 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 payments 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.

**Keywords:** E-commerce, Internet payment, public key cryptography, security, on-line travel agency

## 1. Introduction

Internet invents a new style of life. It breaks the physical barriers of time and space, so that people can go around the world without leaving home. Editors of the National Geographic Traveler Magazine [1] elect cyberspace to be one out of fifty places that travelers should visit in their life time. Most importantly, customers can buy goods or make monetary transactions through the World Wide Web since E-commerce booms nowadays.

For the transactions performed in Internet in an electronic form, we need a secure Internet payment system to handle the transactions. Criteria include security, cost, time and capacity should be carefully considered when an Internet payment system is introduced.

Section 2 presents the proposed Internet payment model which is designed for an online electronic commerce application. Section 3 presents TravelNet, an online Web application integrated with the proposed payment model. Section 4 presents an evaluation of the security and performance of the whole system. Section 5 presents the conclusion of this paper.

## 2. Payment Model

We propose an Internet payment system. The proposed system simulates the buying behavior of customers who use a credit card or cash card to buy goods. The procedure of buying goods in our payment system is the same as that in a real life.

Our main focus is on the purchasing part (how customers interact with merchants) and the payment process (how money is settled down). Four major entities involved in our system. They are customers, merchants, a payment gateway and banks. Before we describe our payment system, we introduce the conventions that are used in the message content.

- 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 two types of credit card: MasterCard (MC) and VISA (VS).
- e_date: The expiry date of the 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 acknowledgement 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,

[†] The work described in this paper was supported by a grant from the Research Grant Council of the Hong Kong Special Administrative Region (Project No. CUHK4432/99E).

denoted by X.

- 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 1: Conventions used in the message content of our payment system*

The mechanism of the payment model is shown in Figure 1. The details of the information flows are as follows:

i. After the customer finishes choosing the products from the merchant's homepage, a secure connection between the customer and the merchant is established using SSL [2] protocol for information transferring. The customer information as well as the product information will be packed together and sent to the merchant web server. The message content (MC1) in this step is

**MC1:** *{card_name, card_no, e_date, card_type, address, prod_id, quan, amt, p_opt}*$_{\mathit{by\ SSL}}$

ii. Upon the receipt of message MC1, the merchant get the product and the customer's information. The merchant then requests for payment authorization from Issuer and payment capture from Acquirer. A message (MC2) which consists of the customer's personal and the merchant's information, is sent to the payment gateway (PG). This message will be encrypted twice by the merchant's private key and then the PG's public key. At this step, the message packet (MC2) is

**MC2:** *{{card_name, card_no, e_date, card_type, amt, m_name}*$_{\mathit{merc\_priv}}$*, m_id, SIG, p_opt}*$_{\mathit{pg\_pub}}$

iii. When the PG receives the message (MC2) from the merchant, the PG uses the corresponding keys to decrypt the message. Next, the PG will communicate with the Issuer and the Acquirer through an existing banking network. After the PG receives the acknowledgement, the PG will compose a message (MC3) including the acknowledgement and a receipt to the merchant for record purposes. This message is also encrypted twicely by the PG's private key and then the merchant's public key. The message content is

**MC3:** *{{RESULT, receipt, m_name}*$_{\mathit{pg\_priv}}$*, SIG, pg_cert}*$_{\mathit{merc\_pub}}$

iv. Upon the receipt of the PG's message, the merchant will decrypt the message to obtain the plain message. After verifying the result, a message (MC4) is composed to inform the customer whether the purchase is successful. 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}*$_{\mathit{by\ SSL}}$

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

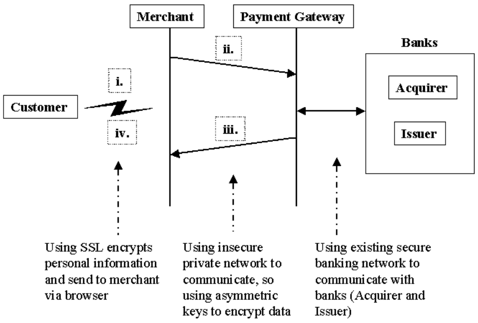
Merchant
Payment Gateway
Banks
Acquirer
Issuer
Customer
i.
ii.
iii.
iv.
Using SSL encrypts personal information and send to merchant via browser
Using insecure private network to communicate, so using asymmetric keys to encrypt data
Using existing secure banking network to communicate with banks (Acquirer and Issuer)

*Fig. 1: The Payment System and Its Payment Process Flows*

We have described a light-weight payment system for E-commerce applications. The system is faster yet secure to handle the personal information from being stolen by malicious users. Descriptions on how the system is secure from attacks are given in section 4. The payment system is implemented and incorporated into an online travel agent system called TravelNet for testing and performance evaluation.

## 3. TravelNet

TravelNet is a project that simulates a real life E-commerce application, i.e. an online travelling agency. There are similar E-commerce applications in the web, for example, Expedia [3] and Travelocity [4]. TravelNet is an Web application [5] and it provides services like flight reservation, travel accessories selling, tour guides, and hotel reservation. Secured payment [6] will be done by the payment system mentioned in the previous section and the credit card payment is provided by TravelNet.

The overall architecture of TravelNet is shown in Figure 2. Details of the information flow are described as follows:

i. A client communicates with a merchant server through HTTP on the SSL layer. Information from the client like orders and user authentication will be passed to the merchant. Through this channel, the merchant can push responses back to the client.

ii. The merchant server accesses local user profile database for authentication, updating, inserting new users, etc. We implement the merchant server by Servlets [7, 8]. The main advantages of Java Servlet are the great concurrent performance and platform independent nature. Users are not able to view the source code of the programs (for cracking or hacking purposes) from the exposed object code. Consequently, security is provided on the server.

iii. The merchant server accesses its local inventory stock database for getting product information or updating inventories.

iv. The merchant server consults foreign companies (e.g. flight companies in TravelNet) for product information query, booking, ordering, etc.

v. Connected to the payment gateway (PG), the merchant server requests a payment from a specific credit card. Message to PG will be encrypted by an agreed public key of PG and TravelNet's private key will be used for authentication (MC2). An acknowledgement of a successful or unsuccessful transaction will be encrypted by TravelNet's public key and send back from PG to TravelNet (MC3).

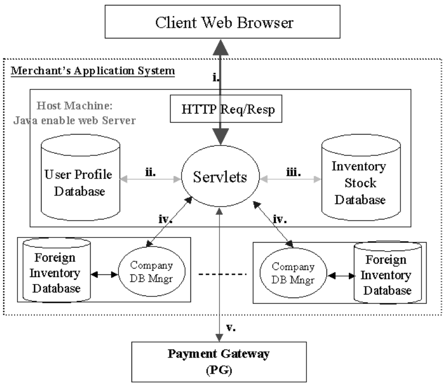

*Fig. 2: The Overall Architecture of TravelNet*

## 4. System Evaluation

In this section, we evaluate the design of our payment model which is incorporated in TravelNet.

### 4.1 Qualitative Analysis

For a system to be secure from potential attacks, it should handle the attacks on eavesdropping, message tampering and masquerading. TravelNet and the payment system are secure from those attacks.

With public key cryptography, attackers cannot see the contents of the message (MC1, MC2, MC3 and MC4) if they do not have the corresponding keys to decrypt to obtain a plain message. Hence, eavesdropping is avoided.

Any encrypted message cannot be tampered with, since it will not be possible to decrypt it after it has been changed. By using message digests, a digitally signed message cannot be tampered with. In MC2 and MC3, digitally signed messages are used to prevent message tampering attack.

TravelNet system gets a server certificate from a trust third party for authentication purpose. Masquerading is consequently prevented on the system. Moreover, messages are authenticated with a digital signature to prevent masquerading.

Comparing with the performance of the SET protocol, our system is faster in terms of the number of symmetric keys generated. In the SET protocol, the number of symmetric keys generated is six while our proposed system does not require any.

### 4.2 Performance Measurement

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 checkout 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 5 executions to obtain the average time measure for each data point in every experiment.

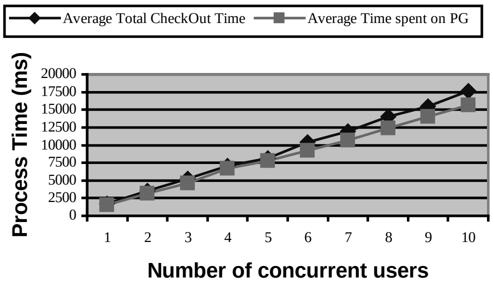

*Fig. 3: Payment Transaction Time in Multiple-Threaded Model*

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. There is also an extra task switching overhead that is very significant when the number of tasks becomes large. As displayed in Figure 3, the payment process time increases as the number of concurrent users increases. Besides, 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 checkout process, payment server contributes over 80%.

In the single-threaded model, TravelNet clients request in a first-come-first-serve manner. Figure 4 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 5 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 have to be shared among the multiple requests, the requests will hold resource (e.g., lock a data item) and compete with each other, thus delaying the complete time. 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.

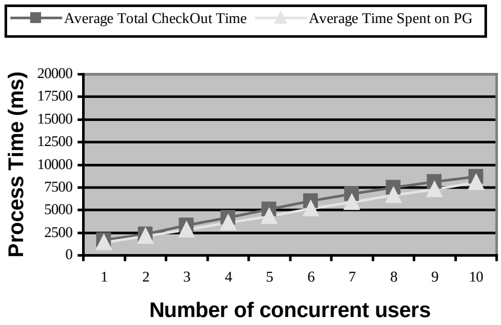

*Fig. 4: Payment Transaction Time in Single-Threaded Model*

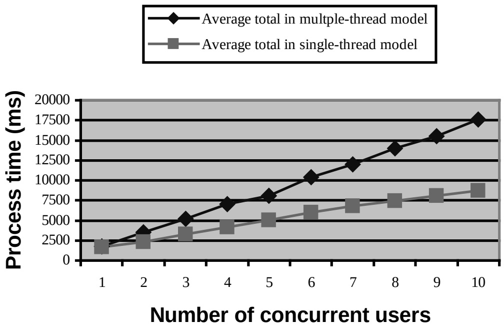

*Fig. 5: A Comparison for Single-Threaded and Multi-Threaded Model*

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 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.

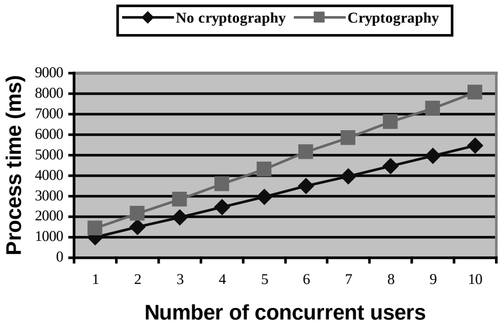

*Fig. 6: Single-Threaded Model on the Payment Transaction Time on PG*

## 5. Conclusions

Payment system is an essential component in the Internet electronic commerce. We propose a light-weight payment system, in comparison with the complicated SET protocol. To test and evaluate the payment system, we build an online travel agency called TravelNet, which simulates a real-life E-commerce application. Performance evaluation is conducted and the results show that our payment system is secure and cost-effective. In the future, we will simulate the SET protocol in TravelNet and evaluate the performance between these two approaches.

REFERENCES

1. *50 places of a lifetime*, National Geographic Traveler Magazine, Special 15th Anniversary Issue
2. Alan O. Freier, Philip Karlton, Paul C. Kocher, *The SSL Protocol Version 3.0*, Internet Draft, March 1996.
3. *Expedia.com*, http://expedia.msn.com
4. *Travelocity*, http://www.travelocity.com
5. *Web Application Development*, http://www.winwinsoft.com/articles/wad.html
6. *Security in Internet Transaction*, http://www.holt.ie/text/security.html
7. *Web Application Development*, http://www.winwinsoft.com/articles/wad.html
8. C. Darby, *Developing 3-Tier Database Apps w/ Java Servlets*, Java Developers Journal, Feb 1998, http://www.sys-con.com/java/