Internet Payment Methods: Mechanism, Application, and Experimentation

Term 3 report

prepared by

Chong Ka Lung
(98080070)

Supervisors:
Prof. Michael, R. S. Lyu
Dr. Y. S. Moon

Markers:
Prof. Ada, W. S. Fu
Prof. John, C. S. Lui

December 4, 1999.

Department of Computer Science and Engineering
The Chinese University of Hong Kong

Abstract

In this paper, an Internet payment system is proposed. It gives users a choice to choose which payment method they like to use, either credit card or electronic coins. A literature review on existing payment systems and cryptography are discussed in the beginning of the paper. Then we discuss the mechanism of the proposed system and comparisons between the existing systems and the proposed one. At last, we will discuss the usages of the payment system in real life.

Contents

1 Introduction

Cyberspace was elected to be one out of fifty places of a lifetime travelers should visit in the life time. It was elected by editors of National Geographic Traveler Magazine [1]. It concludes that Cyberspace is one of the world wonders and a place easy to accessible for travelers. From the economical point of view, the market size is huge, any economic activities can play a success in the Internet. Therefore, there appeared many different electronic commerce applications worldwide.

The Internet invents a new style of life. It breaks the physical barriers of time and space, so that you can roam around the world without leaving home. Most importantly, you can buy goods or make monetary transactions through the world wide web. The main difference is using mouse and keyboard for buying compared with traditional behavior, which you pay for the goods in shop.

When we talk about payment systems, there are four major elements which we should always bear in mind: (1). the parties involved; (2). the means of payment; (3). the medium of exchange; and (4). the infrastructure handling the transaction. The parties involved can range from banks or financial institutions, individuals, non-bank corporations, to computer software providers. The means of payment include currency and bank deposit. The medium of exchange will include instruments such as cash, credit cards, checks, or bills. The infrastructure handling the transaction can be ATMs and POSs, check and bill clearing system, and Internet banking. They are common to most of the payment systems all over the world.

For the transactions doing in the 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 of customers and make use of those information to buy another goods for them. Therefore, to prevent fraud and disputes, entity authentication of the parties, message integrity protection and non-repudiation of payment order should be included in the system. How many parties involved in the payment process is also a factor to affect the security of the system.

- **Cost**: The cost of the payment order should be bigger than the cost of the payment system. Cryptography is used to encrypt the critical information before it is transmitted to the network. A higher security is acquired by a complexed cryptographic algorithm. However, the level of security depends on the cost of goods/services. That is, a higher security is used to perform higher transaction cost and vice versa; otherwise, the cost of the goods will be doubled when compared with the shop prices. In all, there is a golden rule that the cost of the payment system should be less than the cost of the goods/services.

- **Time**: The time of the payment process should be reasonably fast, otherwise, no customer was going to wait for the payment process in a long time manner. It is crystal clear that the efficiency of the system depends on the computation time as well as the cost of the payment. Number of parties involved in the payment process also influence the time of the system.

- **Capacity**: The capacity of the system is how many people can use it concurrently. In other words, maximum people use the system to do purchasing online without any failure or overloading of the system.

In this paper, we present an Internet payment system satisfying the requirements of the above criteria. The remainder of this paper is organized as follows. Section 2 presents some existing payment systems used in the Internet nowadays. The architecture on different payment systems are discussed. Besides, an introduction on cryptography and also cryptographic terms such as symmetric-key system, public-key system, digital signature, message digest, and public-key certificate are discussed. Section 3 describes our electronic payment system. The architecture, features and also the message contents of different states in the system are discussed. Section 4 gives a qualitative analysis on our system compared with the existing systems. Section 5 introduces some targeted applications which will make use of the payment system. Section 6 presents some future works which will be carried out in the coming semester. A short summary is discussed in Section 7.

2 Related work

There are many wellknown protocols, and existing electronic payment systems implemented by commercial companies working in the Internet. Pre-registration of user is required in most cases. Online payment is the usual approach to deal with Internet payment, credit card or account PINs will be sent over Internet with more or less security protection in many cases. There are many approaches to solve the problems.

2.1 Existing payment systems

Internet Keyed Protocol (iKP) [13] 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 [17].

Secure Electronic Transaction (SET) [12] was incorporated by MasterCard and Visa. It images electronic commerce built on the CA-based security. The SET includes a payment section, which is able to deal with different credit cards. The SET applies acquirer payment gateway which 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 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 ciphermessage. 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 (SSL) Protocol [2] was developed by Netscape Communications Corporation. It provides privacy and reliability between two communicating applications. The protocol is composed of two layers. At the lowest level, layered on top of some reliable transport protocol (e.g., TCP), is the SSL Record Protocol. The SSL Record Protocol is used for encapsulation of various higher level protocols. One such encapsulated 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 them can be found in [15].

Qudro-way Internet Payment Protocol (QIPP) [10] is a simple yet secure electronic payment for the electronic market on the World Wide Web. The Protocol imitates the conventional payment in a shop. There are four parties involved: customer, merchant, payment gateway and certificate authority. It is different from most other payment systems, the payment will be initiated by the customer, 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.

The DigiCash [4] is invented by Belgian-based US cryptographer David Chaum. It uses public-key cryptography techniques to assure anonymity and it is an on-line electronic cash system. The DigiCash system aims to provide the privacy of customers, based on blind signature [3]. 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. Becauser the bank has no idea of the blinding factor, it has no way of linking the note numbers that 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 grow enormously and quickly. This greatly affect the performance of the system.

NetCash [7, 8] 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.

There are other payment protocols which 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 [5] system is based on a close examination of systems such as NetCash, Ecash and other related systems such as Magic Money [16] and Netbill [11, 9]. It 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 CyberCash [6], Millicent [14], PayWord and MicroMint [19] which are also wellknown.

2.2 Cryptography

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.

As the Internet and other forms of electronic communication become more prevalent, electronic security is becoming increasingly important. Cryptography is used to protect credit card information and personal information when electronic shopping and online registration are held.

Cryptography systems can be broadly classified into two types: (1). symmetric-key systems; and (2). public-key systems. For symmetric-key system, encryption and decryption key are the same and must be kept secret. For public-key system, the encryption key is dfferent from the decryption key. The encryption key can be made public whereas the decryption key has to be kept secret. Encryption is the function, which encrypts arbitary messages with encryption key while decryption function is to recover the message into its original form from its encrypted form by using the decryption key.

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 [18] public-key system. It was developed by three scientists: Ron Rivest, Adi Shamir and Leonard Adleman in 1977.

There are three other important concepts which are crucial to a secure electronic commerce: Digital signature, Message digest, and public-key certificate. Digital signatures are 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, at a later time, repudiate the signature. 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 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.

A public-key certificate 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.

In our proposed system, RSA public-key cryptosystem, digital signature, message digest and also public-key certificate are used in order to provide a secure payment system.

3 The System

An Internet payment system is proposed. The proposed system is similar to the buying behavior of a normal customer who uses a credit card or uses coins to buy goods. The procedure of buying goods on our payment system is similar to the buying behavior in real life.

The system provides two payment options: credit card or electronic coin. Customers with or without a credit card can also make online transaction. Therefore, they can use their credit card to buy the goods or use electronic coins which bought from the bank in order to make a transaction in the World Wide Web. The conventional shopping choice is preserved. That is, customers first browse the goods in the merchant shop (Internet), then they pick up those required goods (put into cart). They bring the goods to cashier (charge out) and the transaction is complete after they pay for the goods (payment system). They can pay either by credit card or by cash (electronic coins). This provides a greater flexibility for the user.

Most people can use our system without any difficulties providing that they own a credit card or an existing bank saving account. Our target users are those often using computer browsing the World Wide Web.

In use of our system, there are advantages on:

- Give choices on payment method
- Provide some degree of privacy and anonymity
- Provide a simple secure payment system
- Unchanged shopping habit for customer

There are four major entities involved in our system. They are customer, merchant, acquirer (it has the merchant's account) and bank. The Certificate Authority will manage the certificate and those public keys of the entity. RSA public-key cryptography is used for authentication and encryption purposes. A pair of private/public keys is being generated by the customer itself or by the trusted third party, i.e. Certificate Authority.

Our main focus is on the purchasing part (how customers interact with merchants) and the payment process (how money are settled down). Other issues such as how the keys will be managed and distributed to the users are not our concern.

Besides, there is an general assumption that it is secure from attacks in the communication network between acquirer and the existing banking system.

Actually, credit card and electronic coin are two payment approaches in the Internet payment. We start by discussing the mechanism on the credit card, then discussing the mechanism on the electronic coin approach. In addition, the message contents used in our credit card and electronic coin payment system are described. Then, there is a description on how both systems are combined.

The following conventions are used in describing the message content:

- acc_no: The customer's bank account number.
- address: The mailing address of the customer.
- amt: The total amount of the purchased goods.
- bank_receipt: An acknowledgement is sent to the customer from the bank for the buying of COINS and it serves as a record to the customer.
- 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).
- COINS: The electronic coins. It consists of the value of the coins, serial number of the coins, the bank identification number (bank_id) and the date of issuance.
- e_date: The expiry date of the customer's credit card.
- i_date: The issue date of the serial numbers of COINS.
- 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 from acquirer to merchant, and also from merchant to customer, stating whether the transaction is completed or aborted.
- serial_no: A sequence of numbers denoting the serial number of the COINS.

- SIG: The digital signature of a message. It uses the sender's private key to sign on an message digest.
- X_cert: A public-key certificate of different parties X. It is composed of the acquirer's name, the public-key, trusted third party's name. X = acquirer (acq) and 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 = acquirer (acq), bank (bank), customer (cust), or merchant (merc).
- X_pub: The public key of party X. X = acquirer (acq), bank (bank), customer (cust), or merchant (merc).

3.1 Credit card payment

Figure 1 shows the mechanism of our credit card payment system. the details are as follows:

1. Customer browses the merchant shop and searches his favorite products. When he found it, he put the goods into a virtual cart or basket which holds all the information of the products. When he finishes browsing the products, he will trigger the payment process by choosing the payment methods, either credit card payment or electronic coins payment.

   A secure connection between customer and merchant is established using SSL protocol. Customer enters his personal information and credit card information into the browser. In addition, product information and the total amount will be included in the message which sent to merchant.

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

2. Upon the receipt of message, merchant can get the personal information and credit card information of customer. He will then compose a message which consists of customer's personal and credit card information, together with the total amount and merchant's name. This message will be encrypted by merchant's private key to serve as authentication. The message then attachs to a header which contains the merchant identification number and a number denotes the payment option customer chose. The whole message is encrypted with acquirer's public key and it serves as privacy that no body except acquirer can decrypt it to get a cleartext. At last, merchant will send out the

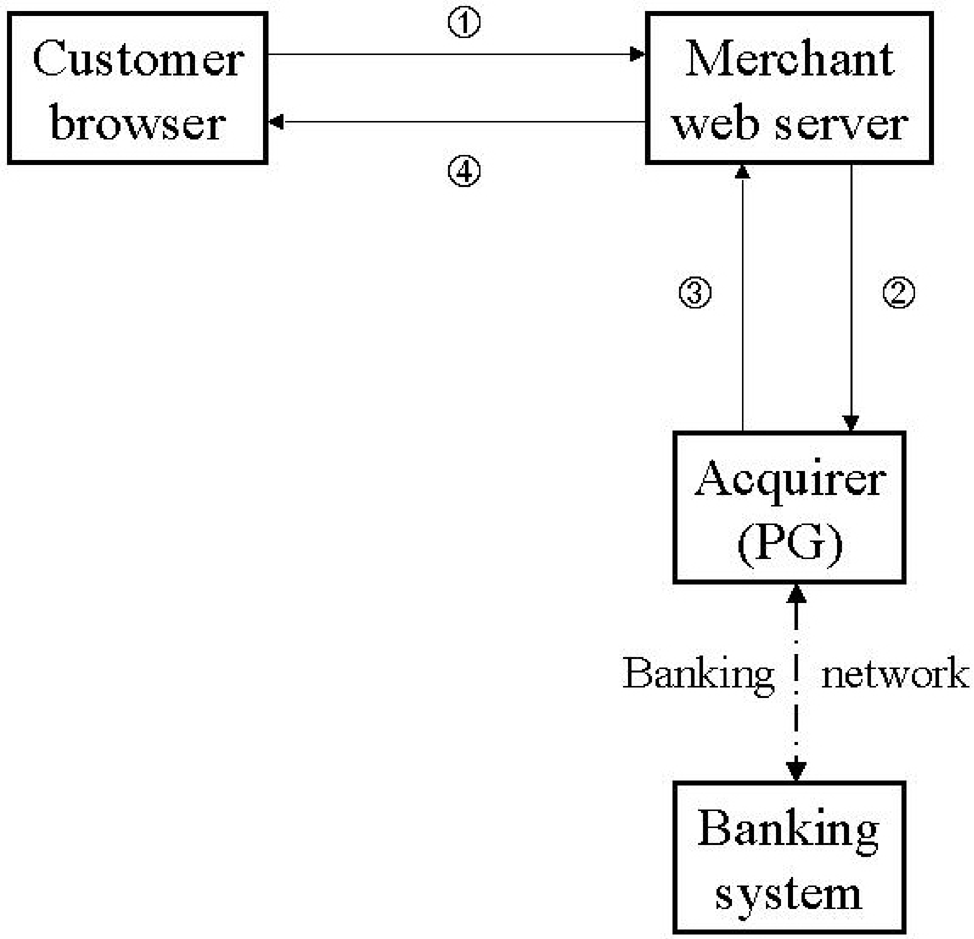

Figure 1: Mechanism on credit card payment

message packet to acquirer for verification and validation of the credit card. Besides, merchant asks acquirer to settle the money for himself.

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

3. When acquirer receives the message from the merchant, he first uses his private key to decrypt the message to get a decrypted message and a header. Then, he will notice the message is sent by a specific merchant which only his public key can decrypt the message. Next, acquirer will communicate with the issuer (the bank issue customer's credit card) through the existing banking network which assumes it is secure. After the acquirer receives the response from the issuer, it will compose a message including the response (whether the credit card is valid and not over credit limit or vice versa) and a receipt to the merchant for record purposes. It is then encrypted by ac-

quirer's private key for authentication. In addition to the message, acquirer's certificate is adhered to the message and together encrypted by merchant's public key for privacy purpose.

Message: $\{\{RESULT, receipt, m\_name\}_{acq\_priv}, SIG, acq\_cert\}_{merc\_pub}$

4. Upon receipt of the acquirer's message, merchant will decrypt the message using his private key and then using acquirer's public key to obtain the original message. After checking the result, merchant will compose a message to inform the customer if the purchase is success or failure. The message will be shown as a html document.

   Message: $\{RESULT, receipt, prod\_id, quan, card\_name, address\}$

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

3.2 Electronic coin payment

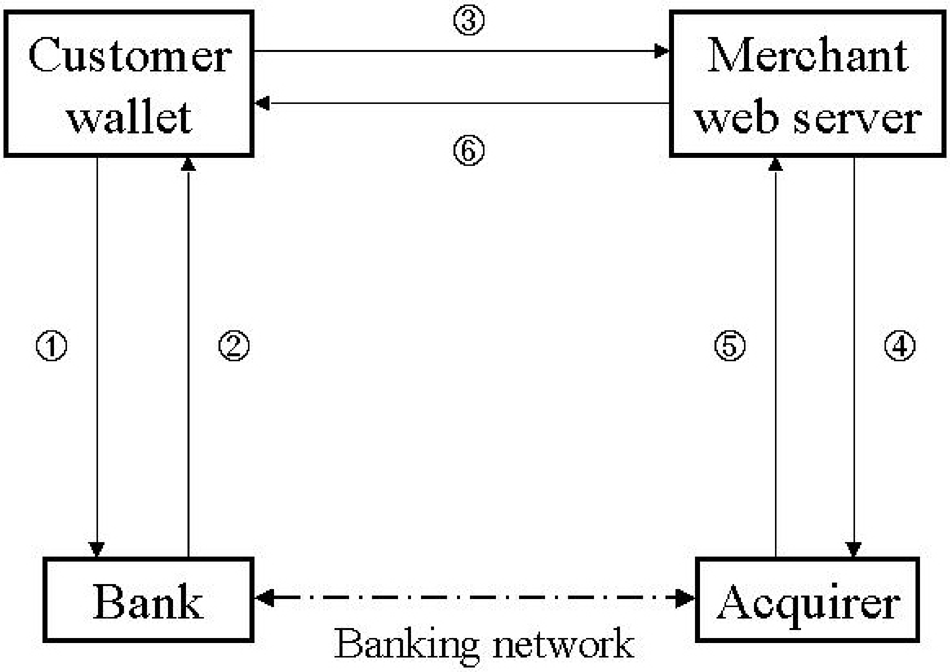

Figure 2: Mechanism on electronic coin payment

A special client software is used to store electronic coins which are bought from the bank. It achieves some extent of anonymity. Figure 2 shows the mechanism on electronic coin payment system. The details are as follows:

1. Customers have to activate the first and second operations for buying electronic coins from the bank before their first payment using electronic coins.

   Customer needs to download a special software to store electronic coins and to buy the coins from bank. The customer transfers his money from his saving account into electronic coins which they will be stored in the software resided in the customer's computer. A message is comprised to make the request of buying coins. It consists of his saving account number, bank identification code and amount to be transferred. Then it is encrypted by his private key and then by bank's public key to achieve privacy and authentication purposes.

   Message: $\{\{acc\_no, bank\_id, amt\}_{cust\_priv}, SIG, cust\_name\}_{bank\_pub}$

2. After the message is received by the bank, it will use his own private key to decrypt the message to get a newly decrypted message and a string denotes the customer's name. Then the customer's public key is chosen to decrypt the message and get all message contents. So the bank will check whether if the requested amount is over the amount in the saving account. If the money in the saving account is more than requested, electronic coins will be made and transferring to the customer; otherwise, the process is aborted and a failure message will be sent to customer.

   The reply message is composed of those electronic coins, a bank receipt stating the time when the transaction takes place and amount of money involved. It is encrypted by bank's private key and then in addition to the bank's public-key certificate. The whole message is encrypted again by customer's public key so that no one can view the contents without customer's permission.

   Message: $\{\{COINS, bank\_receipt, amt\}_{bank\_priv}\}, bank\_cert, SIG_{cust\_pub}$

   The electronic coins are composed of the book value, the issuance bank identification code, the serial number of all coins and the issuance date.

   $COINS$: $\{amt, i\_date, bank\_id, serial\_no\}_{bank\_priv}$

3. In the following four operations are purchasing process using electronic coins.

   This time, the customer selects the electronic coin payment option instead of credit card payment option, the special software will be executed automatically. It will compose a message to the merchant. It consists of product-id, quantity, amount and coins. It is encrypted by merchant's public key for privacy.

   Message: $\{COINS, amt, prod\_id, quan, p\_opt\}_{merc\_pub}$

4. Upon receipt of customer's message, it is decrypted by merchant's private key to obtain the cleartext. Then, it forwards the coins in addition to a message comprised the merchant name and the total amount to the acquirer. The message is encrypted by merchant's public key. After that a header stating the merchant identification code will be attached to the encrypted message and encrypted once more by using acquirer's public key.

   Message: $\{\{COINS, amt, m\_name\}_{merc\_priv}, m\_id, SIG, p\_opt\}_{acq\_pub}$

5. When the acquirer receives the encrypted message, he first decrypts it and gets the plain message. Then it communicates with the bank who issued the coins for verification of double spending of coins. Acquirer can get the information who is the issuing bank from the coins message. Next, acquirer will wait for the reply from the issuing bank. When acquirer receives the response from the issuing bank, it composes a message to the merchant stating the result of the payment process. The message will be encrypted two times by using acquirer's private key and then by merchant's public key for authenticating and privacy purposes.

   Message: $\{\{RESULT, receipt, m\_name\}_{acq\_priv}, acq\_cert, SIG\}_{merc\_pub}$

6. Upon receipt of the acquirer's message, merchant will decrypt it using his private key and then using the acquirer's public key obatined from the certificate to decrypt the included message to obtain the original message. After checking the result, merchant will compose a message to inform the customer if the purchase is success or failure. The software will keep a record on the transaction.

   Message: $\{RESULT, receipt, prod\_id, quan\}$

Customer will choose any one of the payment options when they proceed to checkout the items. After they select the one, different mechanism will be executed according to their selection.

In our proposed system, it can be divided into several small systems which resides in different places. They are the special wallet software, the merchant system and the acquirer system (payment gateway system).

4 Qualitative Analysis

Our system is secure from attacks such as eavesdropping, message tampering and masquerading. An attacker cannot see the contents of the message because the message is encrypted with the public key of the recipient. Only the private key can decrypt the message.

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.

Messages are authenticated with a digital signature prevents masquerading. It is because a digital signature uses owner's private key. No other people will own the private key except the owner. Therefore, masquerading can be prevented using digital signature technique.

In analysis of the existing payment systems, we divide into different aspects: (1). complexity of credit card payment; (2). complexity of electronic coin payment; and (3). message flow used.

1. **Complexity of credit card payment**: There is a similarity in the systems using credit card payment. Most of them use a trusted third party or certificate authority to authenticate all parties involved in the payment process and to manage all the keys and certificates. In our system, we use SSL protocol to make a secure connection between customer and merchant. Although the credit card information might be stolen by some employees of merchant's company and no privacy to the credit card information, the time spent will be lower in our system because of less communications between many parties. Consensus is easy to make when the number of parties involved is small.

   It uses the complicated cryptographic algorithm to make the whole system secure for doing transaction in the Internet. For example, in SET protocol, there are two pairs of key exchange keys: encryption keys and signature keys. It is difficult for crackers to crack the system. However, it is time-consuming and storage-consuming in order to achieve the highest security. In our system, security is our concern, but not in a complicated way and not to achieve the highest security. The system is secure from attacks at least on eavesdropping, message tampering and masquerading.

2. **Complexity of electronic coin payment**: In the electronic coin payment, it is not as complex as credit card. An important issue is double spending of the coins. How can we prevent from this attacks? Our system follows the idea of NetCash to prevent double spending by minting coins into a database when electronic coins are bought. It prevents maintaining a large database when the system grows.

   Also it is not so complicated in our electronic coin payment. It provides certain level of anonymity which similar to the behavior of using coins in real life with anonymity feature.

3. **Message flow used**: The message flow used in the payment system would influence the time spent and the cost of the payment system. In our system, we use less messages in the payment process between involved parties which is less than other existing payment system.

5 Target Applications

5.1 TravelNet

TravelNet is a project that simulates real life e-commerce application, i.e. an online travelling agency. TravelNet will provide friendly interface and fancy features to the users. Apart from application level, security issue and integration with nearly real-life payment system using visa cards will be another major concern for our system. In TravelNet, the application provides services including flight reservation, travel accessories shopping, travel guides and hotel reservation.

The implementation between client-server will be different from the commonly used CGI nowadays. Java servlet will become our replacement for CGI. This server side Java provides better performance, easier to be incorporated with database and distributed components and its platform independence. Security issue is another important part of the system, so popular SSL protocol and the RSA algorithm will be practised in it.

As a whole, TravelNet tries to practise the real-life e-commerce model in addition to some new technologies. More detailed description will be followed.

5.1.1 The architecture

- **The overall architecture is described as followings:**

  1. The web server will collect Http Requests from the client web browser to our host machine. All the data transmission between web client and web

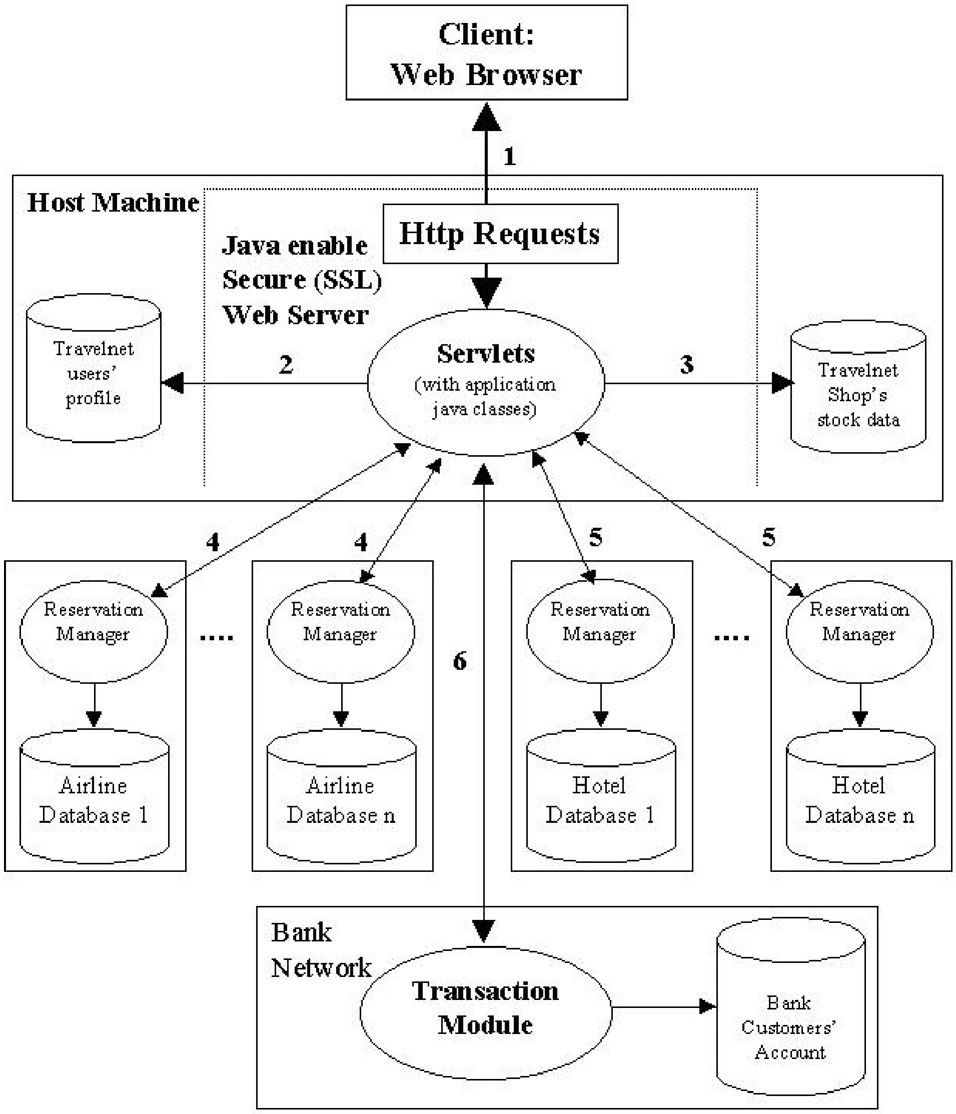

Figure 3: The architecture of TravelNet

server is on the *Secure Socket Layer (SSL)* in order to keep the user's information to be protected. Response to an Http request may simply return a HTML document. The request may have to be processed by our server side program (JAVA Servlets), and then response will be given back in HTML format.

2. TravelNet users' database can be accessed by server servlets (or some applications chained with servlets). The main purposes are data retrieval or update of TravelNet users' profile like username, password, address, phone number etc...

3. TravelNet shop database is for storing the necessary detail of the selling items. These detail can be achieved by our server so as to process client requests.

4. TravelNet server can connect to any one of the authorized airline-companies' servers (reservation manager) for querying flight information or reservation of tickets. An acknowledgement will be return to our server to indicate the status of the request.
5. TravelNet server can connect to any one of the authorized hotels' servers (reservation manager) for querying available room information or reservation of rooms. An acknowledgement will be return to our server to indicate the status of the request.
6. Transaction (debit from user's credit card account) can be done by sending request to the bank transaction module. Meanwhile, the requests can be a validation of credit card. Successfulness of the transaction or validation will acknowledge our server. Valid requests will result in update of the bank database of corresponding user's account

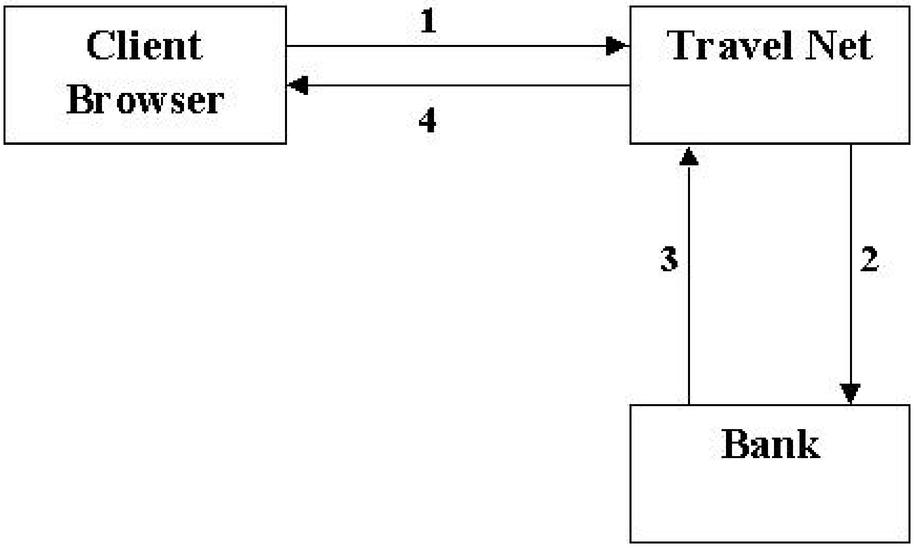

Figure 4: The payment mechanism of TravelNet

- **Payment in TravelNet by credit card**

  1. A client requests to checkout what he/she planned to buy. This request will activate our server to process payment procedure.
  2. User's information are encrypted before sending to the bank. User's credit card information will be validated and if the credit card is valid, the requested amount will be deducted from the specific user account.
  3. A successful or unsuccessful transaction acknowledgement will be sent back to TravelNet server for us to ensure whether the client request is valid or not.

4. Client will receive a response, indicating whether their request is successful or not. HTML code will be the format for response.

5.1.2 Features of TravelNet

There is a number of features implemented in TravelNet to ensure that a complete range of travelling service can be provided to its users.

- **Flight Reservation Service**: This is the service which allows users to query on the price and availability of certain flights, which will make query on the associated airline flight database by the information that is supplied by the users. For a successful query, user should supply some basic information about the nature of the flight so that the agent can retrieve correct information from the airline databases.

- **Travel Shop**: Travel shop provides the necessary stuffs for travel. It's simply an online shop. Our customers can shop what they need on our web by clicks. Desired items can be put in their electronic shop basket and can be check out any time in their login session. Once a customer checked out, credit will be deducted from their account and the product will be delivered to customer's address by our courier.

- **Bank**: Payment is a key element in all e-commerce systems, and it is also the case for TravelNet. Strictly speaking, the entity Bank here is not part of the online travel agent but it is responsible for performing a complete online transaction. Therefore it is also implemented for the whole transaction in the right track. As mentioned before in the part of discussing the architecture, the bank is responsible for validating the credit card information from users and grant payment to the agent later. Therefore, two functions as discussed in the architecture part are provided by the bank to the agent so that all internal validity process and the transfer of payment process are abstracted from the travel agent.

- **Membership**: Users are required to register a free membership before using the reservation service and the shopping service. The idea is that it helps to block away for unauthorized transaction of any payment service. Also, it allows the agent to maintain better customer service. For example, the agent can notice its member for any news on discounted products. For a complete membership service to be provided, it allows new member registration, change of member information for existing membership, list of itinerary of the member, member login and logout. Note that any credit card information is not required in registration process. When using the reservation service or the shopping service, members are required to login first. The login process requires the users to input their user name and the password which are distributed to them during their registration of their membership. Once they have login, they are free to use the service until they have logout. Since some users will forget to logout when they finish their operation, the system will automatically logout for a certain period of idle session exhibited by the users.

A secure payment system is a critical component in this application. Due to the transaction doing in worldwide and a large amount of money flow are estimated, the payment system have to be secure enough. Also, additional security technique such as SSL is used when the customer is entering personal information and credit card information via the client browser such as Netscape Navigator and then transferring to the merchant side.

5.2 Mondex

Mondex is an application of a smart card system. The card have to link to a bank account. It contains memory and a processor for transferring money from your bank account into the card and vice versa. Also the card can be used for making transaction via a hardware equipment, card reader, which reads the card information and modify the amount of money stored into the card.

Our proposed payment system can make use the smart card system for transaction instead of entering information into the browser by customers. It is time saving for the inputting process when smart card is used. However, a special hardware is needed for reading the smart card.

5.3 Mobile clients

We use mobile clients to denote those handheld equipments such as Personal Digital Assistant (PDA). For example, PalmPilot. In making use of the mobility and easy to carry characteristics, it is good for them to act as a digital wallet to store cash. Through the IrDA port or a cable connecting the digital wallet with a computer, you can use the Internet payment system from anywhere. This is the major advantage of mobility.

The application uses a IrDA port to make a connection between the digital wallet and the payment system. The amount stored in the digital wallet is debited. Moreover, if the digital wallet is a PDA, it can serves more functions, not just only a wallet.

6 Future work

The proposed Internet payment system will be implemented in the coming semester. The whole system includes the payment gateway which is the intermediary between the merchant and the bank. After the system is implemented, then we will incorporate it into other online electronic business applications to carry out experiments. Experiments such as determining the performance and the capacity of the system will be run.

Mobility is an important issue nowadays. Everything is going into movable such as mobile phone, notebook, palm PC, handheld PC. We will try to incorporate the proposed payment system into those mobile equipment such as personal digital assistant (PDA) so that it acts as a wallet and stores cash in it without carrying lot of cash. Analysis on the system itself will also be carried out.

7 Conclusion

Payment system is an essential component in the Internet electronic commerce. A new payment system is proposed which provides two choices to customers, either using credit card or using electronic coins, to pay the amount of transaction. Combining both payment methods provides a flexibility to the customer.

The proposed system is designed which consists of the merits of the existing systems. It is secure from being attacks and privacy problems. The system can incorporate into the Internet business application, the smart card system such as Mondex, and also the personal digital assistant which many people use nowadays.

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, http://home.netscape.com/eng/ssl3/3-SPEC.HTM

[3] D. Chaum, *Blind Signatures for Untraceable Payments*, Advances in Cryptology: Proceedings of Crypto 82, Plenum Press, 1983, pp. 199-203.

[4] Chaum D., Fiat A., Naor M., *Untraceable Electronic Cash*, Advances in Cryptology CRYPTO' 88, S. Goldwawwer (Ed.), Springer-Verlag, pp.319-327.

[5] Donal O'Mahony, Michael Peirce, *Scaleable, Secure Cash Payment for WWW Resources with the PayMe Protocol Set*, http://ganges.cs.tcd.ie/mepeirce/Project/Payme/Overview.html

[6] Eastlake 3rd, D., et al., *CyberCash Credit Card Protocol Version 0.8*, RFC 1898, Feb. 1996

[7] Gennady Medvinsky and B. Clifford Neuman, *Electronic Currency for the Internet*, Electronic Markets Vol.3 No.9/10, October 1993, pages 23-24.

[8] 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, November 1993.

[9] J. D. Tygar, *NetBill: An Internet Commerce System Optimized for Network Delivered Services*, Carnegie Mellon University, Pittsburgh, Pennsylvania 15213, 1995.

[10] J. Zhao, C. Dong and E. Koch, *Yet Another Simple Internet Electronic Payment System*, Proc. of the IFIP 1996 World Conference - Mobile Communications (Canberra, Australia, Sept. 1996).

[11] Marvin Sirbu and J. Douglas Tygar, *An Electronic Commerce System Optimized for Network Delivered Information and Services*, In Proceedings of IEEE Compcon '95, March 1995.

[12] MasterCard International - What is SET?, http://www.mastercard.com/shoponline/set/set.html

[13] 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.

[14] MilliCent Microcommerce System, http://www.millicent.digital.com/

[15] Y. S. Moon, H. C. Ho, *Secure Transport Protocol for E-Commerce - SET versus SSL*, Multimedia Information Systems in Practice, edited by Wing S. Chow, Springer.

[16] Product Cypher, *Magic Money Digital Cash System*, ftp://ftp.csn.org, 1994.

[17] Ralf Hauser, Michael Steiner, and Michael Waidner, *Micro-Payments based on iKP*, December 17, 1995.

[18] R. L. Rivest, A. Shamir, and L. Adleman, *A method for obtaining digital signatures and public-key cryptosystems*, Comm. ACM, vol.21, no.2, pp.120-126, 1978.

[19] R. L. Rivest, A. Shamir, *PayWord and MicroMint: Two simple micropayment schemes*, http://theory.lcs.mit.edu/˜rivest/RivestShamir-mpay.ps