A Novel Shopping Protocol for Ubiquitous Commerce

Iuon-Chang Lin and Hsiao-Chi Chiang

Abstract—Due to the prosperity of ubiquitous computing and mobile communication technologies, the traditional commerce will start changing drastically. A shopping model has shown how the customers make a purchase from before-shopping to post-shopping through a ubiquitous device. However, the ubiquitous computing system gathers the sensitive personal information such as location and credit card information. Therefore, security and privacy have become important issues which should be taken into account in the system. In order to solve these problems, this paper tries to design a helpful and secure ubiquitous shopping protocol which is combined with the shopping model to make it practical, secure, and convenient.

Index Terms—Payment, privacy, security, ubiquitous commerce.

1. Introduction

Due to the popularity of Internet information technology, the commerce has progressed from electronic commerce to ubiquitous commerce. The concept of ubiquitous computing was proposed by Weiser in 1992[1]. Traditional commerce is restricted to physical marketplace, but nowadays, people can process transactions through the Internet. Although electronic commerce is a popular transaction at the present time, there are still many problems and potentials needed to be improved[2]. In the electronic commerce age, service providers focus on how to convert service content into digital content so that users can receive those digitized content using information and communication technology (ICT) and equipment. In the mobile commerce age, customers are able to receive digitized services anywhere. Therefore, the mobile service providers make effort to enhance platforms reachable to mobile devices. In the ubiquitous commerce environment, service providers intend to provide customers with any commerce services via any devices so as to enable customers to finish related transactions anywhere at anytime[3]-[8].

In the traditional shopping transaction, customers need to enter into shops to make a purchase. Nowadays, customers prefer shopping through the Internet to visiting stores physically. In the current shopping circumstances, general customers cannot compare the price of products among different shops so that they are not sure if they get the best price or not. The concept of ubiquitous shopping model was first introduced by Qi et al.[9] in 2010. The shopping model shows how customers make the purchase from before-shopping to post-shopping through a ubiquitous device. However, the ubiquitous computing system gathers much sensitive people’s private information such as location and credit card information. Therefore, security and privacy problems should be taken into account in the system. In order to solve these problems, this paper tries to combine the shopping models and design a helpful and secure ubiquitous shopping protocol.

This paper is structured as follows. Section 2 presents related works focusing on designing a payment system. Section 3 describes the architecture of ubiquitous devices for shopping. Section 4 introduces a ubiquitous shopping protocol. The security analysis can be found in Section 5. Finally, conclusions are presented in Section 6.

2. Related Works

M. Weiser[1] described that the ubiquitous computing system was seamlessly integrated into user’s daily life in 1992. After that, lots of application systems were proposed, but the security and privacy in such environment have not been studied deeply. Since the ubiquitous computing system collects and keeps much sensitive information of people, the security and privacy issues should be taken into account in the system design[10]. If personal current location information or detail location history is let out to others, it may cause severe threats.

Both location information and personal transaction information should be protected. Cheng et al.[11] proposed the mobile ubiquitous privacy protection for electronic transactions (MUPPET), a privacy-aware information brokerage framework, which combines some novel techniques to prevent users’ private information from release.

According to [12], there are several security issues that need to be taken into account in the ubiquitous computing system. In particular, the following requirements are critical to design a ubiquitous computing payment system[13]-[17].
2.1 Security

Obviously, security is an important problem in any payment system and sufficient protections have to be taken against frauds such as theft, forge money, and payment denial. In the ubiquitous commerce environment, since services are provided via any device anywhere at anytime, it is more vulnerable to security breaches compared with the physically secured and controlled environments.

2.2 Privacy

Many payment systems require users to disclose personal information such as their names and credit card numbers as parts of the transaction. But in some scenarios, users do not want to disclose this information to pay for services or goods. Furthermore, payment systems must have adequate privacy protection mechanisms. Thus, to be accepted by users for payment systems, privacy should be considered.

Due to the ubiquitous commerce being evolved from mobile commerce, there is a similar model in the payment system. According to the mobile payment forum (MPF)[11], the mobile payment model includes the customer, the merchant, the mobile operator, and the payment transaction processing. The mobile operator can be divided into mobile network operator, financial instructions (such as bank, credit card issuer), government (laws and policy institute), service provider, software provider, and device manufacturer.

3. Architecture of Ubiquitous Device for Shopping

The ubiquitous computing is operated on the ubiquitous devices, and the computing result is provided from the service provider. The proposed module by [4] can be integrated into our protocol. According to the shopping module[4], the purchase process consists of three different activities: before-shopping, during-shopping, and post-shopping. Fig. 1 shows the shopping computing modules, which are described in the following.

A. Before-Shopping: the Stage that Consumers Begin to Think over Buying Something.

1) According to consumers’ requirements, provide products information. For example, if a consumer wants to buy a mobile phone, “mobile phone” could be the key word to be input into the ubiquitous device. The system would provide goods information like HTC, iPhone, Sony Ericsson, etc. Besides, the system also provides consumers with the comparison of different products.

2) According to input geographic information, provide location suggestions. After deciding to buy iPhone, the next step is to know the shop’s location. Consumers send geographical range information to the related geographic information system (GIS) by a ubiquitous device, and then the location suggestion would respond to consumers.

B. During-Shopping: the Stage that Consumers Enter the Shop and Make a Purchase Decision.

1) Obtain product information according to radio frequency identification (RFID). When a consumer enters the shop, he could inquire the ubiquitous device for product information according to the tag involved in the products.

2) Price comparison with nearby shops. After deciding what to buy, consumers could inquire different prices in nearby shops through the ubiquitous device. It can help consumers to negotiate prices with shops and make a better decision.

C. Post-Shopping: Payment and Logistics after Selecting the Goods. After-Sale Service also Should be Considered.

1) Mobile payment with the ubiquitous device. After choosing goods, customers must pay for them. They can choose ways of payment, such as e-cash or credit card. In order to integrate conveniently, the ubiquitous device could also connect to the online bank through wireless networks.

2) Logistics selection according to GIS. The ubiquitous device could use GIS to provide information to the consumer. If you buy a heavy item, the ubiquitous device could provide suitable choices of location and traffic.

3) Record and reminding of the service or maintenance information. Some goods need after-sale service or maintenance. The ubiquitous device could record the service or maintain necessary information. When they come to the service or the maintenance expiration date, the ubiquitous device will remind the consumer.

4. A Ubiquitous Shopping Protocol

4.1 Notations for Protocol Description

We introduce some notations needed to be used in the ubiquitous shopping protocol, as shown in Table 1.

![Fig. 1. Shopping computing module.](image-url)
The proposed ubiquitous shopping protocol can be divided into four phases: 1) the registration phase, 2) the before-shopping phase, 3) the during-shopping phase, and 4) the post-shopping phase.

A. Registration Phase

Before using the ubiquitous shopping protocol, the customer has to register in the bank and the service provider. The merchant has to register in the service provider.

Customer \longleftrightarrow Service provider

Step 1: The customer sends his identity ID_C to the service provider.

Step 2: Service provider computes \( K_{C} = MAC(\text{ID}_C, K_{SP}) \), where \( K_{SP} \) is the service provider’s secret key, and then sends \( K_C \) to the customer to be customer’s secret key.

Merchant \longleftrightarrow Service provider

Step 1: The merchant sends his identity ID_M to the service provider.

Step 2: The service provider computes \( K_{M} = MAC(\text{ID}_M, K_{SP}) \) and then sends \( K_M \) to the merchant to be merchant’s key.

Step 3: The merchant sends the P_ID, P_NAME, and P_PRICE, which encrypt with merchant’s key to the service provider. The merchant changes the product information to the service provider regularly.

Customer \longleftrightarrow Bank

Step 1: The customer sends his identity ID_C to the service provider.

Step 2: The service provider computes \( K_{C_B} = MAC(\text{ID}_C, K_B) \), where \( K_B \) is bank’s secret key, and then sends \( K_{C_B} \) to the customer to be a session key between bank and customer.

B. Before-Shopping and During-Shopping Phase

When the customer wants to make purchases, he requests a purchase suggestion from the service provider. The steps of this phase are specified as follows (refer to Fig. 2).

Step 1: The customer encrypts the requirement information (RI) with customer’s key \( R = E_{K_C}(\text{RI}) \), where RI includes customer’s coordinates, requirement, and hobbies. And then sends R and ID_C to the service provider. For example, the customer wants to buy a white iPhone, and he is located in a shopping mall. The customer sends the information \( E_{K_C} \) (coordinates, iPhone, white) and his identity ID_C to the service provider.

Step 2: When the service provider receives the request, the customer key can be obtained by computing \( K_C = MAC(\text{ID}_C, K_{SP}) \). Therefore, the service provider can decrypt the message, and obtain coordinates, requirement, and hobbies. After that the service provider will know what the customer wants to buy, and then give suggestion to the customer. The service provider uses customer’s key to encrypt the product information and ID_M, and then sends the message to the customer. Product information includes P_ID, P_NAME, and P_PRICE. For example, the service provider sends the white iPhone information, and then sends the white iPhone information and product information to the customer’s ubiquitous device. In the meanwhile, the service provider provides the price comparison among nearby shops.

Fig. 2. Before-shopping and during-shopping phase.
C. Post-Shopping Phase

After customers get the suggestion information and decide which one to buy, they can use the ubiquitous device to pay for goods to the merchant M. The following steps are performed (refer to Fig. 3).

Step 1:
1) The customer encrypts the Pl with the session key between customers and banks, \( P_{\text{IK}} = E_{K_{\text{IK}}} (\text{Pl}) \), where Pl includes ID\(_C\), TID, transaction amount, and e-cash or credit card number.
2) The customer encrypts the order information (OI) with the customer’s secret key \( O_{\text{IK}} = E_{K_{\text{IK}}} (\text{OI}) \), where OI includes ID\(_C\), ID\(_M\), TID, product ID, product price, and amount.
3) The customer computes \( V = \text{MAC} (K_C, P, O, T) \).

Step 2: The customer delivers the \( P, O, V, \text{IDC}, \) and \( T \) to the service provider.

Step 3: The service provider checks \( V \) to ensure the \( P \) and \( O \), which receives from the customer are correlated pairs. And the service provider checks whether \( T \) is in a valid time or not.

Step 4: The service provider delivers ID\(_{\text{SP}}\), ID\(_C\), TID, and \( P \) to the bank. Here, the bank just needs to know the payment information to deduct money from the customer’s account, but the bank does not know the order information, thus it can protect the customer’s privacy. The service provider and the bank are communicated through the secure channel.

Step 5: When the bank receives the ID\(_C\), it can compute \( K_{C,B} \) to decrypt \( P \). According to \( P \), the bank can deduct money from the customer’s account.

Step 6: Bank sends an acknowledgement to the service provider to acknowledge that the payment has succeeded.

Step 7: The service provider decrypts the \( O \) with \( K_C \) to know who is the merchant with ID\(_M\), and then encrypts the new order information OI’ with merchant’s key \( K_{M,} \) where OI’ includes TID, ID\(_M\), P ID, P NAME, P PRICE, and amount. The purpose for the service provider to eliminate the ID\(_C\) is that he/she wants to protect the customer’s privacy.

Step 8: The service provider forwards OI’ to the merchant, and tells the merchant whether the payment has been finished or not. And then the merchant prepares the goods purchased by the customer.

Step 9: When the merchant finishes the purchase, he delivers an acknowledgement to inform the service provider that the purchase has succeeded. In the meantime, the merchant also delivers MI encrypted with \( K_M \) to the service provider, where MI includes TID, P ID, ID\(_M\), M_DATE, and the service provider records it to his database. When it comes to the maintenance day, the service provider will remind the customer through the ubiquitous device.

Step 10: The Service provider delivers an acknowledgement to inform the customer that all payment phases have succeeded and finished. In the meanwhile, the service provider also provides the reasonable choices according to the item location and traffic situation.

<table>
<thead>
<tr>
<th>C</th>
<th>SP</th>
<th>B</th>
<th>M</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Compute ( P = E_{K_{\text{IK}}} (\text{Pl}) ), ( O = E_{K_{\text{IK}}} (\text{OI}) ), ( V = \text{MAC} (K_C, P, O, T) )</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. ( P, O, V, \text{IDC}, T )</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Check ( V )</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. ID(_{\text{SP}}), ID(_C), TID, P ( P ) ( \text{SP} )</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5. Decrypt ( P ) with ( K_C = \text{MAC} (ID_C, K_b) ) according to ( P ), deducts money from customer’s account.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6. Ack.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7. Decrypt ( O ) with ( K_C ) to know ( ID_M ), ( \text{Compute } O = E_{K_{M}} (\text{OI'}) )</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8. ( O' )</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9. Ack., ( E_{K_{B}} = (LI) )</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Fig. 3. Post-shopping phase.

5. Security Analysis

In this section, we will demonstrate the security of the proposed ubiquitous shopping protocol. The security analysis involves two aspects: privacy, and authentication and integrity.

5.1 Privacy

Because the credit card number or e-cash is encrypted by the customer and bank’s session key \( K_{C,B} \), it can keep confidentiality from being transferred over the ubiquitous computing. Therefore, the ubiquitous shopping protocol ensures that the e-cash or credit card number is not leaked. In addition, the payment information only forwards to the bank. The merchant knows the order information (what the customer has purchased), but he does not know the detail of the payment information (the e-cash or credit card number). On the contrary, the order information only forwards to the merchant. The bank just knows the payment information (the e-cash or credit card number), but he does not know the detail order information (what the customer has purchased). The result shows that the ubiquitous shopping protocol can protect the privacy of customers.

5.2 Authentication and Integrity

In the proposed ubiquitous shopping protocol, we assume that the service provider is a trusted party. The keys of customers and merchants are generated by the service provider using the message authentication code. Without the service provider’s secret key and message authentication code, no one can obtain the customer’s key and merchant’s key to decrypt the messages. Therefore, except for the trusted service provider, the key \( K_C \) or \( K_M \) is only held by the corresponding customer or merchant. In the same way, without the bank’s secret key and message authentication code, no one can obtain the session key between customers and banks to decrypt the messages.

6. Conclusions

In this paper, we have presented a ubiquitous shopping
protocol that relies on ubiquitous devices. A customer can search information by using the ubiquitous device to make a purchase. This protocol provides not only convenience, but also security. Even if someone obtains the message, the customer need not worry the purchase information will be leaked. Therefore, this protocol can be used in the real world.

References


Iuon-Chang Lin received the B.S. degree in computer and information science from Tunghai University in 1998 and the M.S. degree in information management from Chaoyang University of Technology in 2000. He received his Ph.D. degree in computer science and information engineering in March 2004 from National Chung Cheng University. He is currently an associate professor with the Department of Management Information Systems, National Chung Hsing University. His current research interests include electronic commerce, information security, cryptography, and mobile communications.

Hsiao-Chi Chiang was born in Taiwan in 1987. She received the B.S. degree in information management from Yuan Ze University in 2010. Now she is a student with National Chung Hsing University. Her current research interests include electronic commerce, information security, e-business system, and security of e-commerce.