Online Real-Time Credit Card Processing Models

Mohammad A. Rob
School of Business and Public Administration
University of Houston-Clear Lake
Houston, Texas 77058, USA
rob@cl.uh.edu

Sanwar Ali
Computer Science Department
Indiana University of Pennsylvania
Indiana, Pennsylvania 15705, USA
sanwar@iup.edu

Abstract

Although a variety of payment mechanisms have been developed over the years for online businesses, payment by credit cards remain the leading mechanism for online payments. For real-time online credit card processing, a merchant needs to install a third-party proprietary software in the merchant e-commerce server. However, many issues need to be resolved before integrating a third-party payment solution to a merchant e-commerce system. In this paper, we attempt to address the current state of the online real-time credit card processing models. We also discuss several factors such as cost, complexity and security issues related to implementing such a system.

1. Introduction

Over the past few years, many dot-com companies have failed; however, e-commerce is stabilizing to those companies that streamlined their online business processes [6]. According to a recent report [2], purchase of goods and services over the Internet is expected to increase from $325 billion in 2001 to nearly $3.5 trillion in 2006. The consumer spending of e-commerce for the year 2003 is estimated to be at $110 billion [16]. Despite poor economy in recent years, online consumer shopping has increased from 2001 to 2002 by 43% [7]. During the 2002 holiday season, online consumers spent $367.05 million on December 8 – an all-time high for one-day shopping; the weekly spending was about $2 billion [8]. NACHA, the electronic payment association which develops operating rules of the ACH network, the largest network of electronic payment processors in the United States, introduced a new payment category for WEB transactions in 2001 [1]. According to their latest report, WEB transactions increased more than 300% from 2001 to 2002. Consumers are also increasingly embracing electronic methods of payment [18][21].

In the traditional retail business, the display of products, processing of payments, and delivery of goods are handled by merchants in front of the customers. In the e-commerce arena, these processes are typically handled by three different parties, and payment over the Internet is the most common concern for the consumers. Between 40 to 60 percent of Internet purchases are abandoned in the midstream, because customers do not want to compromise privacy or the security of their financial information [12]. To address these issues, various online payment mechanisms have been developed that include: digital cash, electronic wallet, electronic check, and smart card. Most of these mechanisms have failed due to the complexity of use and implementation as well as poor customer trust. Thus, payments by credit cards remain the most prevalent mechanism for online consumer payments [13] [25].

A complete e-commerce business cycle requires interactions between several hardware and software components physically located in different geographical locations. An electronic merchant usually develops and maintains the merchant processes, while the financial institutions or software companies provide payment services to the merchants. However, in most cases, payments are not processed in real-time. For reasons of security, complexity, and cost, the payment information is typically collected from a consumer but is processed off-line like a physical store. For real-time payment processing, a merchant needs to install a third-party proprietary software in the merchant e-commerce server. However, many issues need to be resolved before integrating a third-party payment solution to a merchant system – the most important is the technical knowledge of the people who are developing the e-commerce system. For large companies, this may not be an issue, but for small companies where resources are limited, it is important to understand the challenges of implementing an online credit card processing system.

This paper attempts to address the current state of the online credit card processing system. First, we provide an overview of the credit card processing mechanism. We then focus on the various models of online, real-time credit card processing system and discuss several factors such as cost, complexity and security issues related to implementing such a system. The results can be extremely valuable to small businesses that are venturing into Internet commerce.

2. Credit Card Processing Mechanism

There are in general six parties involved in a traditional credit card processing cycle: customer, card issuing bank, merchant, merchant's bank, acquirer, and a credit card processor. The card issuing bank issues credit cards to customers and maintains their accounts. The merchant opens an account with a bank to receive payments. In order to accept credit cards, the merchant needs to register with an acquirer – a bank or financial institution that sets up an account for the merchant and provides a terminal to process credit cards. The processor is a large data center maintained by the credit card

network, and it acts as a clearinghouse for all credit card transactions.

There are two stages of transactions for any credit card purchase: payment authorization and fund capture. Authorization refers to checking the account number to see if it is still valid, has sufficient credit, and has not been reported lost or stolen. Capture refers to approval and posting of the transaction and shipment of goods. When a purchase is made by a customer, the merchant uses the terminal to send payment information to the acquirer. The acquirer contacts the card processor for authorization, which in turn contacts the customer's bank for credit availability, and if all goes well, provides a charge authorization number to the acquirer. The acquirer transmits back the authorization to the merchant. All transactions happen in few seconds and no transaction of money takes place yet.

To capture funds, the acquirer accumulates multiple payment authorizations and submits them as a batch to the processor on an hourly or daily basis. After receiving the fund, the acquirer deducts a small fee and credits the rest to the merchant's bank. Thus, all the costs associated with the credit card processing are borne by the merchants. The process of refund follows a similar set of transactions.

The credit card processing mechanism was developed by the financial institutions over a long period of time. The fundamental method of payment authorization and capture of funds are the same whether the purchase is made from a physical store or via Internet. However, the biggest hurdle for an online merchant is to get the credit card and personal information from the customer securely over the Internet

The online payment processing becomes further complicated due to the introduction of a payment gateway that replaces the acquirer or acts in between the merchant and the acquirer. It is typically a software company or a financial institution that provides necessary software to the merchant for real-time payment processing. Most banks will not set up a merchant account for an online business because online businesses are classified high risk.

3. Methods of Credit Card Processing

A merchant can process credit card payments in a number of ways. These include manual entry through a touch-tone telephone, manual entry using a point-of-sale (POS) terminal, manual or electronic entry via a PC acting like a POS terminal, or electronic entry from a Web site [23]. Many of these mechanisms require physical interaction of the merchant with the customer or a system.

For real-time payment processing, an online merchant needs to integrate a payment processing software to the e-commerce site, so that the communication between the software tools used by the customer, the merchant, and the payment gateway are all automated. There are many variations of real-time payment processing, and recent developments include wireless technology with personal digital assistants (PDAs), through which customers can swipe credit cards like traditional POS terminals but complete the payment transaction through the Web [3]. Since there is no standard for the Internet payment processing, a merchant needs to invest some time and money to understand various options and to implement a payment solution suitable for the online store.

4. Online Credit Card Processing Models

Several payment solutions are available for online real-time credit card processing that are implemented through technologies such as standard shopping carts, one-click buy, enterprise e-commerce package, and application service provider. These technologies require installation of some software or modification of Web pages in the merchant e-commerce server. These applications can be grouped into two broader categories of merchant-oriented applications and payment gateway-oriented applications [4][5][14][17].

4.1. Merchant-Oriented Applications

In this case, an online merchant collects customer order information including the product, personal, and credit card, from the e-commerce site, and then forwards the payment information to a payment gateway. The payment gateway in turn communicates with the credit card processor, obtains a charge authorization id to charge the customer account, and sends it back to the merchant Web server. The merchant Web server confirms the order by sending a message to the customer. After fulfilling the order, the merchant requests payments to the payment gateway. Thus, all order and payment transaction data are maintained by the merchant. As most of the processing is performed in the merchant server, these systems are sometimes referred to as local-mode. In this case, the collection of the customer information is via the Internet, whereas the sending of information to the payment gateway can be via phone lines, leased lines, or the Internet. For Internet transmissions, the Secure Socket Layer (SSL) protocol is typically used for data encryption as well as Web Server authentication.

The merchant-oriented applications typically employ a client-server approach as shown in Figure 1. The client software or plug-in is installed in the merchant Web server as a library of programs, usually in C or C++, and the server software, termed as payment gateway, resides with the software provider. The client software is a small messaging agent that uses SSL and X.509 digital certificate technology to securely communicate with the server [24]. The merchant e-commerce system typically pass payment transaction data to the client through a set of name/value pairs implemented in a merchant form at the checkout page. Depending on the fields required by the payment gateway, the code will be different. Various other Web pages and program codes are necessary to handle communication between the customer, the merchant and the gateway.

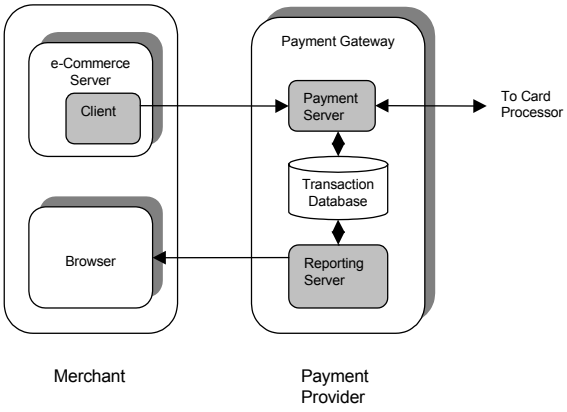

Figure 1: Client-server architecture of Payment Gateway

The payment gateway typically contains a payment server, a transaction database, and a reporting server [10][11]. The payment server accepts encrypted transaction information from multiple clients as well as routes necessary information to the appropriate processing network depending on the credit card. It also performs settlement of transactions. The transaction database contains all transaction-related information for initial orders, payment authorizations, and settlements. The reporting server is used to provide transaction reports such as settled transactions, unsettled transactions, and invalid transactions to the merchant. Thus, in this approach, all order details and some payment information reside in the merchant database, while the payment details reside in the gateway database.

Because most transaction information resides in the merchant's database server, the merchant has more flexibility in the customization of processes and transaction reports, however, strict security protocols must be maintained to protect credit card information in the database. These systems are designed to handle multiple items per transactions, more than 1000 transactions per month, and scalable up to hundreds of millions of transactions. VeriSign's Payflow Pro SDK [24] and Authorize.Net's ADC [3] are examples of merchant-oriented payment applications.

4.2. Payment Gateway-Oriented Applications

These systems are designed for merchants with limited technical capabilities and low transaction volumes. They are typically implemented through a one-click approach and they require minimal changes to the merchant Web pages. The customer usually clicks a link or a button at the checkout page and he or she is directed to a secure page hosted by the payment provider [3][9]. Transaction details (order amount, tax amount, and other parameters) that are encoded in the link are used to initialize the form. The customer then enters credit card details and personal information in the secure form in the gateway Web server.

When the order is submitted, the merchant is notified via e-mail, and the merchant can view specifics of new orders from the Web site maintained by the gateway provider. The processing of payment is same as before; however, all order and payment transactions are maintained by the gateway provider. In this case, the communication between the customer and the merchant is Internet-based, whereas that between the customer and the payment gateway is typically SSL-based. The digital certificate of a single payment gateway serves the customers of all merchants that sign-up with the payment gateway.

The gateway-oriented applications are the simplest payment solutions found in the e-commerce industry, as these systems require less hardware, less technical expertise, and less maintenance for the merchant – these are maintained by the gateway provider. In this case, merchants lose control over the payment transaction data, as they reside with the gateway provider, however, they can view these records through a password-protected Web site hosted by the company providing the payment gateway. A payment gateway provider typically supports many merchants by providing a merchant ID to each merchant and usually helps merchants to open Internet merchant accounts with banks that accept Internet payments by credit cards.

These systems are suitable for merchants processing up to 1000 transactions per month, however, the downside is that only one item can be purchased at a time. VeriSign's Payflow Link [24] and Authorize.Net's WebLink [3] are examples of payment gateway-oriented applications.

5. Issues of Online Credit Card Processing Systems

Selling goods and services on the Internet presents a set of challenges – like how to set up and maintain a secure, reliable, and cost-effective system for payment processing and managing transactions. Several issues need to be resolved before integrating a third-party payment solution to a merchant system – the most important are the security, cost, and complexity.

5.1. Security

The security of financial transactions is of utmost concern when dealing with many parties, especially over the Internet. Consumers must be able to send their financial information to an online merchant without the fear of eavesdropping. They should also be comfortable with the identity of the merchant, that the cyber-merchant is reliable and not bearing a fake identity. The merchant should also be able to send financial information securely to the payment gateway. The technology that addresses these issues is the secure socket layer (SSL) protocol, which uses public- and private-key encryption mechanisms to communicate between a browser and a Web server as well as to authenticate a Web server. If the

merchant is planning for international business, then SSL-encryption key should be 40-bit instead of 128-bit standard for the United States. In order to use SSL, a merchant needs to apply for a digital certificate to a Certification Authority (CA) such as VeriSign [24], get the certificate, and bind it to the IP address of the merchant Web server [20]. The merchant also needs to configure the Web server to accept SSL transmission and develop the payment-related Web pages such that they use HTTPS, the secure version of Hypertext Transfer Protocol.

Fraud prevention such as unauthorized credit card purchase is another important issue for a merchant, because the law provides a consumer liability limit up to $50 if someone uses his/her credit card fraudulently. The merchant is liable for bad transactions – neither the customer, nor the credit card issuer. Thus it is important to use address verification service (AVS) which verifies key components of a customer's shipping addresses against addresses that the credit card issuer has on record for the customer. Research shows that about 65% of the time, criminals using credit card account numbers fraudulently, do not know the account's related billing address [19]. Various other security measures should be implemented for an online purchase, such as, how many times a customer can enter wrong credit card information before it is rejected. In addition, an upper purchase limit to a single transaction or the number of transactions per day by the same credit card number should be controlled.

According to a very recent report [8], about 8 million account numbers of MasterCard, Visa, and American Express credit cards have been compromised from a third-party payment processor. Thus the merchant needs to safeguard the private key used for SSL encryption as well as the consumer privacy information such as credit card numbers and personal data stored in the merchant database. The private key and the credit card number should be stored in the encrypted form, and access to these information should be highly restricted. All sensitive data should be kept behind a firewall and may be in a different database than the one used for the product catalog. To implement these security protocols and to safeguard data requires technical expertise as well as money, both of which might be limited to a small merchant.

5.2. Cost

There are several costs associated with the development and operation of a payment mechanism, and they are all borne by the merchant. Irrespective of the type of payment mechanism implemented, there is always a cost associated either with the development of the payment-related Web pages or integrating the payment software with the catalog pages. This requires in-house technical expertise or consulting service from a payment provider, where the later might cost about $200/hour for a merchant [22]. For merchant-oriented applications, there is also a cost associated with the purchase or lease of the software, and often there are monthly or yearly fees associated with the software license and future upgrades. For payment gateway-oriented applications, commonly there is an application fee, a monthly gateway access fee, and statements fees [15].

There is always an operational cost associated with any credit card processing whether it is performed online or offline. It arises mainly due to the charge placed by the banks and credit card network to process a transaction. Generally, there is a fixed charge for each transaction and a discount rate charged as a percentage of each order-amount. The charges for Internet transactions are often the same as the mail or telephone order transactions, and all of which cost significantly higher than the offline transactions. For example, the discount rate and transaction fee for an Internet transaction are 2.39% and $0.30 respectively, while those for the standard swipe retail are 1.69% and $0.20 [19]. The costs are even higher for international transaction, which are about 3.25% and $0.30, respectively.

The above charges do not significantly vary from one payment provider to another; however, there might be additional charges from a payment gateway if it is not acting as an acquirer. Some payment gateways charge by the volume of transactions, while others provide free transactions up to certain numbers [15]. For merchant-oriented applications, there might be a batch transaction fee and it can run about 10 to 40 cents per batch. There is also a cost for charge back, which is a reversal against a sale that was an error, misunderstanding by the customer, or fraud. It can cost about $10-$25 per charge back [19]. For all non-card present situations such as the Internet, there might be an authorization/verification or AVS (Address Verification System) charge, which might cost about 5 to 10 cents per transaction.

5.3. Complexity

The explosive growth of payment gateways provides a variety of real-time credit card processing options available to an online merchant than can be found for a physical store. For example, all large companies such as Authrize.Net, CyberSource, iTransact, LinkPoint, PaymentOnline, and VeriSign, offer at least three different types of such solutions. In the physical store, the integration of a payment system with an existing point-of-sale system is through a standard hardware/software interface. However, in the online business, the integration is through the software and there is no standard used by various payment gateways.

All online payment applications require certain level of coding and merchant-oriented applications use various technologies such as HTML, ActiveX, ASP, JSP, XML, ODBC, JDBC, or JavaBeans to integrate payment gateways with the e-commerce servers. A merchant must have technical capabilities or means to implement these technologies. Some payment systems are also platform dependent. Thus, integration of a payment system with an existing e-commerce system might be an overwhelming effort, unless a particular payment system is considered during the design phase of the e-commerce system.

Furthermore, all payment systems require testing the whole payment cycle, including the authorization, settlement, and refund, using a valid credit card number.

Another complexity might be due to the level and type of service provided by the payment gateway provider, especially in the case of one-click approach where all transaction data resides with the provider. The merchant is limited by the way the company provides access to the database server, type of search for a particular transaction, refund procedure, audit trails, and statements.

6. Conclusion

We have provided an overview of the credit card processing mechanism and some insight into the real-time online credit card processing systems. Critical factors such as cost, complexity, and security associated with the implementation and maintenance of such systems are also discussed. No matter what method of payment processing mechanism is considered, an online merchant must realize that real-time payment processing can be highly complex – there is no one-size-fits-all solution for all merchants. Whatever payment software is chosen, it needs to be integrated with the e-commerce system, unless one can purchase an integrated e-commerce and payment system. Furthermore, choosing the right payment gateway-provider can relieve a lot of headache of handling payments and interacting with other parties of e-business processes. A payment gateway must support all aspects of payment processing – authorization, capture of funds, refunds, and reports. Products offered by selected vendors should be compared according to the factors such as complexity of the system and software, implementation time and cost, software cost and maintenance fees, transaction costs, and security features for consumers and merchants.

References

[1] ACH, 2002 Electronic Payments Review and Buyer's Guide; *ACH Statistics* (www.nacha.org).

[2] G. Alexander, E-payments in B2B Grow," *Semiconductor International*, January, 2003, 87.

[3] Authorize.Net, Merchant Solutions (www.authorizenet.com).

[4] Authorize.Net WebLink, Linking a web site to the Authorize.Net WebLink secure payment form (www.mktmkt.com/html.htm).

[5] A. Branch, Jr., On the Money: E-Payment Solutions, *University Business*, February, 2002, 31-32.

[6] T. Coltman, T. M. Devinney, A. S. Latukefu, and D. F. Midgley, Keeping E- Business in Perspective, *Communications of the ACM*, Vol. 45(8), 2002, 69-73.

[7] B. Cox, E-Commerce Racks Up $2 Billion Week, (itmanagement.earthweb.com/ecom/print.php/1555371).

[8] B. Cox, Millions of Credit Card Accounts Hacked, *ecommerce-guide.com*, February issue, (ecommerce.internet.com/news/). Downloaded from the Web on February 24, 2003.

[9] CyberCash (www.cybercash.com).

[10] Cybersource, Credit Card processing (www.cybersource.com).

[11] DCTI e-Payment Services, How it Works (www.dcti.com/dcti_pands_howitworks.html).

[12] S. Holly, Internet Business, *PC Magazine*, March 20, 2001, 7-11.

[13] C. Hsieh, E-Commerce Payment Systems: Critical Issues and Management Strategies,"*Human Systems Management*, Vol. 20 (2), 2001, 131-138.

[14] IPOSS Internet Point of Sale System (iposs.creditnet.com)

[15] iTransact, Inc. How it Works (www.itransact.com)

[16] J. Kerstetter, The Internet Economy: Online Payment Plan Evolve, *PC Week*, August 23, 1999

[17] J. Klemow, Credit Card Transactions Via the Internet, *TMA Journal*, Jan-Feb issue, 1999, 11-14.

[18] W. Luo, D. Cook, J. Joseph, and B. Ganapathy, An Exploratory Framework for Understanding Electronic Bill Presentment and Payment Model Selection," *Human Systems Management*, Vol. 19, 2000, 255-264.

[19] MerchantInfoWeb.com, Merchant Account and & Credit Card Processing Information Guide (www.merchantinfoweb.com)

[20] Microsoft Corporation, SSL Mysteries (msdn.microsoft.com/workshop/server/iis/Websec.asp). Downloaded from the Web on February 23, 2003.

[21] J. Patel, and J. Penner, Handling Electronic ill Payments, *Network Computing*, September 18, 2000, 79-88.

[22] Payment Online Corporation, Providing Online Credit Card Processing Solutions (www.paymentonline.com)

[23] G. P. Schneider, J. T. and Perry, *Electronic Commerce*, Course Technology, Cambridge, Massachusetts, 2000.

[24] Verisign, Technical Brief: Building an E-Commerce Trust Infrastructure, SSL Certificates and Online Payment Services (www.verisign.com). Downloaded from the Web on September 25, 2003.

[25] S. E. Weiner, Electronic Payments in the U.S. Economy: An Overview, *Economic Review*, Fourth Quarter, Federal Reserve Bank of Kansas City, 1999, 53-64.