A Secure Way to Payment Gateway Using Mobile

1Yash Paresh Kapadia and 2Amol Joglekar,
1Student, 2Assistant Professor,
1,2Department of Computer Science, Mithibai College, Mumbai, India

Abstract: This paper examines the institutional arrangements in the development of electronic payment system (EPS) and secure electronic payment system for Internet transaction. Payment system plays an important role in the procedure of electronic commerce. This paper presents an analysis of payment system. Based on the research of present status of online payment system on the aspects of mobile application, online payment services for individuals and enterprises, the third-party payment platform, mobile payment, we find some barriers to get in the way of online payment development including lack of central role of commercial banks, payment services unitary, uncertain security and user unawareness. The electronic payment system is to be secure for Internet transaction participants such as Payment gateway server, Bank sever and Merchant server.

Keywords: Debit Cards, Credit Cards, Wallet Payment, Electronic Payment Systems

I. INTRODUCTION

Fund flow has become the most important factor of the procedure of electronic commerce, which is composed of information flow, fund flow and material flow. In today’s business operations, the transfer of money usually means the transfer of control. Electronic commerce has enlarged the scale of payment, which requests the payment system not only to conduct the fund transfer, but also to build a credit platform for all parties who engage in the virtual transactions during the process of corresponding electronic commerce. These payment systems have numbers of requirements: e.g. security, acceptability, convenience, cost, anonymity, control, and traceability. Therefore, instead of focusing on the technological specifications of various electronic payment systems, the researcher have distinguished electronic payment systems based on what is being transmitted over the network; and analyze the difference of each electronic payment system by evaluating their requirements, characteristics and assess the applicability of each system.

A. Data Security

Data security is nothing but to keep all the critical data secure. There are many ways we can encrypt the data. Data can be kept secure by using RSA algorithm. RSA algorithm is nothing must by having two keys one public key and other private key. Public key is shared everyone and private key is kept only with the source. Data is decrypted only when both private key and public key are matched together.

B. Information

Using mobile application transaction can be performed easily also the application user friendly. All parties involved need to pass the encrypted data. No need of landline phone as we have mobile application now.

C. Knowledge

Very basic and simple scenario of card payment only includes 3 parties they are as follows:

1. Payer
2. Payee
3. Transaction Gateway (TG)

Figure 1: Transaction Process

This mobile application of an online store is an important service that keeps the customers of an online company coming back because they view the online store as safe and reliable. In a way also it provides them a sense of safety and security of their financial-transactions.

In order to perform a sale transaction, merchant need to exchange certain information in encrypted form using payment mobile application. If the information is transmitted over the links in plain text, there is a possibility of eavesdropping. Anyone listening to the network traffic could gain access to sensitive information, such as card numbers, card type and whole detail of card holder. Credit card such as a Visa or Master, has a preset spending limit based on user’s credit limit. Debit Cards removes the amount of the charge form the cardholder’s account and transfers it to the seller’s bank. In electronic payment system, server stores records of every transaction. When the electronic payment system eventually goes online to communicate with the shops and the customers who can deposit their money and the server uploads these records for auditing purposes.

For login into the mobile application we need username and password, password is encrypted and saved in database. We need an android application installed on the phone and a dongle which will be inserted in mobile. Using this dongle we can accept card payments. Dongle reads the card data and gives the encrypted data to web service. Web services are used to insert and fetch data from database tables. All the data are encrypted using SHA-1 algorithm. Following are the entities which are involved in the transaction flow:

1. Card Holder’s Bank
2. Merchant Bank
3. Transaction Gateway
4. Vendor Team
5. VISA/Master

Figure 2: Proposed Model
II. LITERATURE REVIEW

Austin Briggs, Laurence Brooks [1] have proposed that this paper examines the institutional arrangements in the development of Nigeria’s electronic payment system (EPS) using a new institutional economics (NIE) perspective. A case study of Nigeria’s EPS was carried out using semi-structured interviews to collect data from 18 participating stakeholders; a thematic method was used for the data analysis. The study suggests that a well-functioning set of arrangements, which is lacking in the institutional setup in Nigeria may be required to build necessary institutional capacity suitable for development of safe and efficient electronic payment systems. Although the technological payment infrastructure in Nigeria is modern and of comparable standard, the failure to put in place reliable and relevant market and collaborative agreements has not enabled full exploitation of the available infrastructure. Current governance structures show elements of power struggle and distrust between stakeholders (players and regulators), hampering the creation of an environment that would sustain free market economic activities and effective development of payment systems.

Xiang Lin[2] have proposed that a payment system plays an important role in the procedure of electronic commerce. This paper presents an analysis of payment system in Wuhan metropolitan area. Based on the research of present status of online payment system on the aspects of portals-construction, online banking services for individuals and enterprises, the third-party payment platform, mobile payment and PSTN payment, we find some barriers to get in the way of online payment development including lack of central role of commercial banks, payment services unitary, uncertain security and users’ unawareness. At last, this paper puts forward some countermeasures to conquer these barriers.

Vorapränee Khu-Smith and Chris J. Mitchell [3] have proposed a growing number of payment transactions are now being made over the Internet. Although transactions are typically made over a secure channel provided using SSL or TLS, there remain some security risks. Meanwhile, EMV-compliant IC cards are being introduced to reduce fraud for conventional debit/credit transactions. In this paper, we propose a way of using EMV IC cards for secure remote payments, such as those made via the Internet, with the goal of providing protection against some of these residual risks. The scheme described in this paper is based on the EMV 2000 Integrated Circuit Card Specification for Payment Systems, which is first outlined. Threats to, and advantages and disadvantages of, the scheme are also examined.

Singh Sumanjeet[4] have proposed that the emergence of e-commerce has created new financial needs that in many cases cannot be effectively fulfilled by the traditional payment systems. Recognizing this, virtually all interested parties are exploring various types of electronic payment system and issues surrounding electronic payment system and digital currency. Broadly electronic payment systems can be classified into four categories: Online Credit Card Payment System, Online Electronic Cash System, Electronic Cheque System and Smart Cards based Electronic Payment System. Each payment system has its advantages and disadvantages for the customers and merchants. These payment systems have numbers of requirements: e.g. security, acceptability, convenience, cost, anonymity, control, and traceability. Therefore, instead of focusing on the technological specifications of various electronic payment systems, the researcher have distinguished electronic payment systems based on what is being transmitted over the network; and analyze the difference of each electronic payment system by evaluating their requirements, characteristics and assess the applicability of each system.

Ajeet Singh, Karan Singh, Shahazad, M. H Khan, Manik Chandra[5] have proposed that in this paper we review a secure electronic payment system for Internet transaction. The electronic payment system is to be secure for Internet transaction participants such as Payment gateway server, Bank server and Merchant server. The security architecture of the system is designed by using Many Security Protocols and techniques, which eliminates the fraud that occurs today with stolen credit card/debit card payment information and customer information. Electronic commerce involves the exchange of some form of money for goods and services over the Internet but today, Internet is an insecure and unreliable media. The asymmetric key cryptosystem Methodology with help of Security Protocol, secure communication tunnel techniques can protect conventional transaction data such as account numbers, amount and other information.

III. RESEARCH METHODOLOGY

Nowadays merchant use landline telephone system and GPRS system for the acceptance of payment. This is a new technique to accept the payment using android application. Also wallet payments are accepted; wallet payment are faster than card payments. Also less security are required in wallet payment. This paper proposes following techniques:

1. Multiple login is supported (Merchant and customer login).
2. Using merchant login card payment can be accepted.
3. Using customer login wallet payment can be accepted.
4. Both customer and merchant can see transaction history.
5. Card data is encrypted using encryption technique.
6. Merchant and need to do complete the sign up process before accepting the card payment.
7. Merchant and customer login is created at the time of sign up process.
8. Login details are saved in sqllite database (mobile database).

IV. PROPOSED ARCHITECTURE

This type of payment system makes it easier for the enterprise merchants also for the acceptance of the card payment. Also the wallet acceptance makes the payment process easier and faster.

1. Sign Up Process:
During the sign up process all the necessary details of the customer and merchant are accepted from the UI. This details are saved in database. Also the details can be fetched from the mobile database. Email Id is the unique ID for the login for both customer as well as merchant.

2. Punch card:
In the punch card holder need to enter the card details like card number, ccv and expiry date. All this data is stored in database. This are the important card details hence the details are encrypted.

3. Swipe card:
For the swipe card merchant need to insert the dongle in headphone jack; after inserting the dongle merchant will swipe the
card holder’s card and accept the card payment using swipe card. Important card details are encrypted using encryption technique.

4. Wallet Payment:
For the wallet payment customer and merchant mobile numbers are required. After entering both mobile numbers just select the wallet type and accept the payment. This is easier and faster way to accept the payment.

5. Security:
Since security is plays an important role in the payment acceptance security is must. Hence the password for login is encrypted using the SHA-1 technique. Card number is saved as masked number. Hence the details are safe and secure.

A. Flow Chart

![Flow Chart of Merchant Login](image1)

![Flow Chart of Customer Login](image2)

B. Algorithm For Encryption

Step 1: Append Padding Bit
Message is “padded” with a 1 and as many 0’s as necessary to bring the message length to 64 bits fewer than an even multiple of 512.

Step 2: Append Length
64 bits are appended to the end of the padded message. These bits hold the binary format of 64 bits indicating the length of the original message.

Step 3: Prepare Processing Functions
SHA1 requires 80 processing functions defined as:
\[ f(t;B,C,D) = \begin{cases} (B \text{ AND } C) \text{ OR } ((\text{NOT } B) \text{ AND } D) & (0 \leq t \leq 19) \\ B \text{ XOR } C \text{ XOR } D & (20 \leq t \leq 39) \\ (B \text{ AND } C) \text{ OR } (B \text{ AND } D) \text{ OR } (C \text{ AND } D) & (40 \leq t \leq 59) \\ B \text{ XOR } C \text{ XOR } D & (60 \leq t \leq 79) \end{cases} \]

Step 4: Prepare Processing Constants
SHA1 requires 80 processing constant words defined as:
\[ K(t) = \begin{cases} 0x5A827999 & (0 \leq t \leq 19) \\ 0x6ED9EBA1 & (20 \leq t \leq 39) \\ 0x8F1BBCDC & (40 \leq t \leq 59) \\ 0xCA62C1D6 & (60 \leq t \leq 79) \end{cases} \]

Step 5: Initialize Buffers…..
SHA1 requires 160 bits or 5 buffers of words (32 bits):
\[ H0 = 0x674523A1 \\ H1 = 0xEF55AB89 \\ H2 = 0x98B4DCC \\ H3 = 0x10325476 \\ H4 = 0xC3D2EA \]

Step 6: Processing Message in 512-bit blocks
This is the main task of SHA1 algorithm which loops through the padded and appended message in 512-bit blocks.
Input and predefined functions:
\[ M[1, 2, ..., L] \]
\[ f(0;B,C,D), f(1,B,C,D), ..., f(79,B,C,D): 80 \]
\[ K(0), K(1), ..., K(79): 80 \]
\[ H0, H1, H2, H3, H4, H5: 5 \]

CONCLUSION
Payment solution for E-Commerce: Card Present, Card Not Present and wallet provides a mobile application solution with multiple login feature for customer as well as merchant for the acceptance of the card payment. This helps the end user by not counting cash again and again. This payment is more secure and also provides the fast and easier way to pay and buy goods.

FUTURE SCOPE
The proposed model will also support EMV cards i.e. it will also support chip and pin cards. At the time of transaction it will ask for the pin entry from the card holder to make the payment even more secured. This is for the card present scenario. Different types of transactions like pre-auth, sale complete, void, refund, cash at pos and purchase with cashback will be supported. In case of card not present an OTP will be sent to card holder mobile number or email to make the payment more secure. In case of wallet payment also it will ask for an OTP from customer...
to make the payment more secure. Also the integration with different wallet provider and banks will be supported. Load wallet will also be done using this application also refund to wallet account will be supported.

References

[4] Singh Sumanjeet, ”Emergence of payment systems in the age of electronic commerce: the state of art”, University of Delhi, India.