Electronic Commerce Application for Mobile and Micro-payment systems

U.S Pandey[1], Kavita[2]
[1]Open learning Delhi University
[2]Singhania University
Pacheri Bari
Jhunjhunu (Rajasthan). India
kavita.yogen@gmail.com

ABSTRACT: *This paper explains that electronic banking uses the computer and electronic technology instead of traditional checks and other paper transactions. The paper relates that electronic commerce in developing countries permit better access to information and marketing opportunities but also have negative aspects such as delays and questionable security. The paper describes the different forms of electronic payment systems and discusses the impact of the internet and electronic cash on the banking system and how we exchange money. The paper also discusses smart card technology and believes that in the future, mobile payment systems and micro-payment systems providing significant convenience to individual customers will lead the way in the development of EPS.*

Keywords: Electronic Payment System, Credit/Debit Card, Smart Card, SET Protocol, SSL Protocols and Security

Received: 11 March 2011, Revised 2 May 2011, Accepted 8 May 2011

1. Introduction

Payment systems that use electronic distribution networks constitute a frequent practice in business sector, especially for banking industry. The term of electronic payments includes any payment to businesses, banks, and public services from citizens or businesses through a telecommunications or electronic network using modern technology. During these years, the important technological payment has developed rapidly. Moreover they created new social practices, which make the use of the payment systems necessary. Electronic payments are as Credit card the most widely used and accepted form of payment, digital wallet provided by Google checkout seems rather cumbersome, stored value payment and who hasn't purchased anything from the PayPal eBay money making monopoly. Electronic cash is a new concept in online payment system because it combines computerized convenience with security and privacy that improve on paper cash. Its versatility opens up a host of new markets and applications. E-cash is an electronic or digital form of value storage and value exchange that have limited convertibility into other forms of value and require intermediaries to convert. Broadly electronic payment systems can be classified into four categories:

1. Online Credit Card Payment System
2. Online Electronic Cash System
3. Electronic Cheque System
4. Smart Cards based Electronic Payment System

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.

Electronic payments involve a payer and a payee. A payer (buyer or customer), is an entity who makes a payment. A payee (seller or merchant), is an entity who receives a payment. The main purpose of an electronic payment protocols is to transfer monetary value from the payer to the payee. The process also involves a financial institution (bank or mint). Typically, financial institution participates in payment protocols in two roles: as an issuer (interacting with the payer) and as an acquirer (interacting with the payee). The issuer is responsible for validating the payer during account registrations and holds the payer's account and assets. The acquirer holds the payee's account and assets. The payee deposits the payments received during a transaction with the acquirer. The acquirer and the issuer then proceed to perform an inter-banking transaction for clearance of funds. It is possible for the issuer and the acquirer to be from the same financial institution.

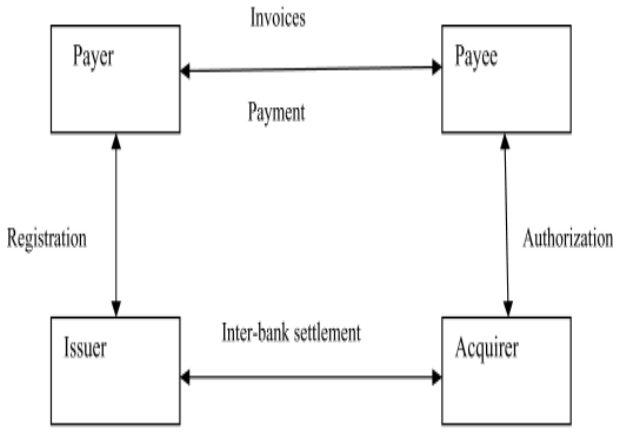

Figure 1. E-payment Protocol

2. Problems with the traditional payment systems

There are many problems with the traditional payment systems that are leading to its fade out. Some of them are enumerated below:

a) Lack or convenience: Traditional payment systems require the consumer to either send paper cheques by snail-mail or require him/her to physically come over and sign papers before performing a transaction. This may lead to annoying circumstances sometimes.

b) Lack of security: This is because the consumer has to send all confidential data on a paper, which is not encrypted, that too by post where it may be read by anyone.

c) Lack of coverage: When we talk in terms of current business, they span many countries or states. These business houses need faster transaction everywhere. This is not possible without the bank having branch near all of the companies' offices. This statement is self- explanatory.

d) Lack of eligibility: Not all potential buyers may have a bank account.

e) Lack of support for micro-transactions: Many transactions done on the internet are of very low cost though they involve data flow between two entities in two countries. The same if done on paper may not be feasible at all.

3. Properties of digital cash

• **Must have a monetary value:** It must be backed by cash, bank authorized credit or a bank certified cashier's check.

• **Must be interoperable or exchangeable** as payment for other digital cash, paper cash, good or services, lines of credit, bank notes or obligations, electronic benefit transfers and the like.

• **Cash could Must be storable and retrievable:**
It stored on a remote computer's memory, in smart cards, or on other easily transported standard or special purpose devices. Remote storage or retrieval would allow users to exchange digital cash from home or office or while travelling.

• **Should not be easy to copy pr tamper** with while it is being exchanged. This is achieved by using the following technologies; these are nothing but new and very efficient versions of the old art of cryptography. Digital cash is based on cryptographic systems called "digital signatures" similar to the signatures used by banks on paper cheques to authenticate a customer. Purchase of digital cash from an online currency server involves 2 steps:

(1) Establishment of an account: in this step we are given a unique digital number, which also becomes our digital signature. As it is a number know only to the customer and the bank, forgery, which may be done in paper cheques becomes very difficult.

(2) Maintenance of sufficient money in the account is required to back any purchase.

4. Types of Electronic Payment

4.1 Online Credit Card Payment System
It seeks to extend the functionality of existing credit cards for use as online shopping payment tools. This payment system has been widely accepted by consumers and merchants throughout the world, and by far the most popular methods of payments especially in the retail markets (Laudon and Traver, 2002). Some of the most important are: privacy, integrity, compatibility, good transaction efficiency, acceptability, convenience, mobility, low financial risk and anonymity. Added to all these, to avoid the complexity associated with the digital cash or electronic-cheques, consumers and vendors are also looking at credit card payments on the internet as one of possible time-tested alternative. But, this payment system has raised several problems before the consumers and merchants. Online credit card payment seeks to address several limitations of online credit card payments for merchant including lack of authentication, repudiation of charges and credit card frauds. It also seeks to address consumer fears about using credit card such as having to reveal credit information at multiple sites and repeatedly having to communicate sensitive information over the Internet. Basic process of Online Credit Card Payment System is very simple. If consumers want to purchase a product or service, they simply send their credit card details to the service provider involved and the credit card organization will handle this payment like any other.

Credit cards, debit cards and prepaid cards currently represent the most common form of electronic payments. For all 3 types of cards the consumer or the business most often uses a plastic card, commonly with a magnetic stripe. The cardholder gives his or her card or card number to a merchant who swipes the card through a terminal or enters the data to a PC. The terminal transmits data to his or her bank, the acquirer. The acquirer transmits the data through a card association to the card issuer who makes a decision on the transaction and relays it back to the merchant, who gives goods or services to the cardholder. Funds flow later for settlement with credit cards and are debited immediately for debit or pre-paid cards. Over time, the chip for payment can be expected to move onto other devices. A "smart card" might then become the computer chip in a phone, PDA or other device that can perform the same function as chip in a plastic card, eliminating the need for the actual plastic card. Smart cards could thus evolve into "smart phones", "smart PDAs" or other "smart" devices.

5. Debit card

Debit cards are also known as check cards. Debit cards look credit cards or automated teller machine (ATM) cards. While a credit card is a way to "play later," a debit card is a way to "play now". When a debit card is used, money is quickly deducted from the related checking or savings account. Debit cards are accepted at many locations, including grocery stores, retail stores, gasoline stations, and restaurants. Debit cards can be used anywhere merchants display the card's brand name or logo. Debit cards offer an alternative to carrying a checkbook or cash. The basic components of ATM machine are carry out the various kinds of transactions like balance enquiry, cash withdrawal, cash deposition, online payments, mini statements & online recharge of prepaid mobile cards of Hutch, Airtel ,BSNL etc. it has the following components like:

• Signage

- Transaction screen
- Card reader
- Receipt printer
- Audio port
- Cassette options
- Envelope options (for cash deposition in some machines)

Debit means "subtract." When a debit card is used, money is subtracted from the related bank account. Debit cards allow only the amount in the bank account to be spent and provide for quick transactions between merchants and personal bank accounts. "online" debit cards are usually enhanced ATM cards that work in the same manner as an ATM transaction , allowing for an immediate electronic transfer of money from a consumer's bank account to a merchant's bank account. To access an account at a store terminal, a PIN must be entered, just as in ATM transaction, giving the system authorization to check an account to see if it contains enough money to cover the transaction. The main advantages of debit cards are:

(a) There is no need to carry cash.

(b) It is quick and less complicated than using a cheque.

(c) It can also be used for withdrawals of cash.

(d) Its holders can have a record of the transactions in his bank statement which will enable him to plan and control the expenditure.

(e) It can be issued to any individual without assessing credit worthiness.

5.1 Electronic Cheque Payment System: Electronic cheque also known as e-cheque and I-cheque are used to make electronic payment between two parties through an intermediary and not very much different from the traditional or current cheque processing system. Electronic cheques are generated and exchanged online. The intermediary will debit the customer account and credit the merchant account. The e-cheque payment system deliberately created to work in much the same way as conventional paper cheque. An account holder will issue an electronic document that contains the name of the financial institution; the payer's account number, the name of payee and amount of cheque. Most of the information is in encoded form. Like a paper cheques e-cheques also bear the digital equivalent of signature: a computed number that authenticates the cheque from the owner of the account. Digital chequing payment system seeks to extend the functionality of existing chequing accounts for use as online shopping payment tools. E-cheque provide a security rich Internet payment option for businesses and offer an easy entry into electronic commerce without a significant investment in new technologies or legal systems.

The process of electronic chequing system can be described using below figure the following steps.

Step 1: a purchaser fills a purchase order form, attaches a payment advice (electronic cheque), signs it with his private key (using his signature hardware), attaches his public key certificate, encrypts it using his private key and sends it to the vendor.

Step 2: the vendor decrypts the information using his private key, checks the purchaser's certificates, signature and cheque, attaches his deposit slip, and endorses the deposit attaching his public key certificates. This is encrypted and sent to his bank

Step 3: the vendor's bank checks the signatures and certificates and sends the cheque for clearance. The banks and clearing houses normally have a private secure data network

Step 4: when the cheque is cleared, the amount is credited to the vendors account and a credit advice is sent to him.

Step 5: the purchaser gets a consolidated debit advice periodically.

5.2 Electronic Cash Payment System: E-cash portability means that it must be freely transferable between any two parties in all forms of e-commerce transactions. In contrast, credit cards do not possess this property of portability or transferability between every combination of two parties. In credit card transactions, the credit card payment recipient must already have a merchant account established with a bank- a condition that is not required with electronic cash.

5.3 Smart Cards based Electronic Payment System: Smart cards are receiving renewed attention as a mode of online payment.

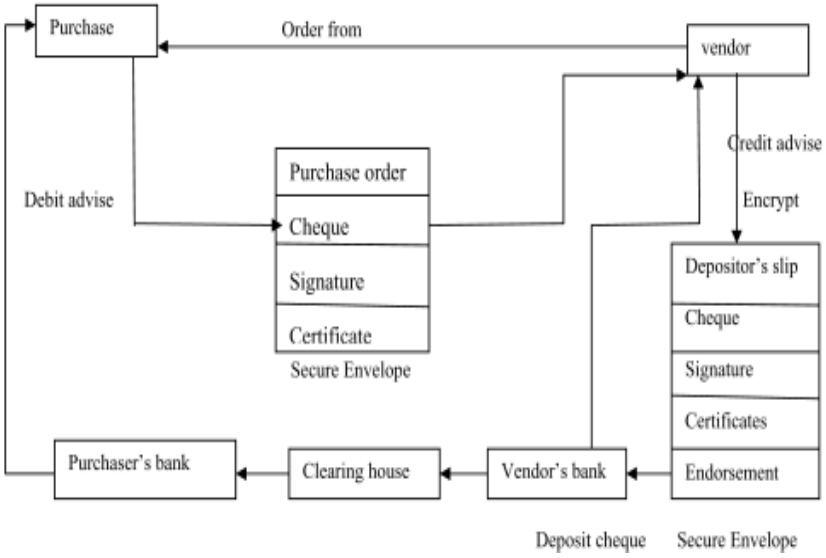

Figure 2. Clearing Cheque payment electronically

They are essentially credit card sized plastic cards with the memory chips and in some cases, with microprocessors embedded in them so as to serve as storage devices for much greater information than credit cards with inbuilt transaction processing capability (Chakrabarti and Kardile, (2002).

6. Internet

Online payments involve the customer transferring money or making a purchase online via the internet. Consumers and businesses can transfer money to third parties from the bank or other account, and hey can also use credit, debit and prepaid cards to make purchases online. Current estimates are that over 80% of payments for online purchases are made using a credit card or debit card. At present, most online transactions involve payment with a credit card. While other forms of payment such as direct debits to accounts or pre-paid accounts and cards are increasing, they currently represent a less developed transaction methodology.

7. Mobile Payments

Mobile phones are currently used for a limited number of electronic transactions. However, the percentage seems likely to increase as mobile phone manufacturers enable the chip and software in the phone for easier electronic commerce. Consumers can use their mobile phone to pay for transactions in several ways. Consumers may send an SMS message, transmit a PIN number, use WAP to make online payments, or perform other segments of their transaction with the phone. As phones develop further, consumers are likely to be able to use infrared, Bluetooth and other means more frequently to transmit full account data in order to make payments securely and easily from their phone.

8. Television Set-Top Boxes and Satellite Receiver

Specialized boxes attached to a television can also be used for payments in some locations. The set-top box attaches to the television and a keyboard or other device, and customers can make purchases by viewing items on the television. Payment is made electronically using a credit card or other account. While usage is presently low, it could grow substantially in countries with a strong cable or satellite television network.

9. Biometric Payments

Electronic payments using biometrics are still largely in their infancy Most biometric payments involve using fingerprints as the identification and access tool, though companies like Visa International are piloting voice recognition technology and retina scans are also under consideration. Essentially, a biometric identifier such as a fingerprint or voice could replace the plastic card

and more securely identifies the person undertaking the transaction. The electronic payment is still charged to a credit card or other account, with the biometric identifier replacing the card, check or other transaction mechanism.

10. Process of Electronic Payment System

Electronic payment systems have been in operations since 1960s and have been expanding rapidly as well as growing in complexity. After the development of conventional payment system, EFT (Electronic Fund Transfer) based payment system came into existence. It was first electronic based payment system, which does not depend on a central processing intermediary. An electronic fund transfer is a financial application of EDI (Electronic Data Interchange), which sends credit card numbers or electronic cheques via secured private networks between banks and major corporations. To use EFT to clear payments and settle accounts, an online payment service will need to add capabilities to process orders, accounts and receipts. But a landmark came in this direction with the development of digital currency. The nature of digital currency or electronic money mirrors that of paper money as a means of payment. As such, digital currency payment systems have the same advantages as paper currency payment, namely anonymity and convenience. As in other electronic payment systems here too security during the transaction and storage is a concern, although from the different perspective, for digital currency systems double spending, counterfeiting, and storage become critical issues whereas eavesdropping and the issue of liability (when charges are made without authorizations) is important for the notational funds transfer. The above figure show that intermediary acts as an electronic bank, which converts outside money (e.g. Rupees), into inside money (e.g. tokens or e-cash), which is circulated within online markets. However, as a private monetary system, digital currency has wide ranging impact on money and monetary system with implications extending far beyond more transactional efficiency.

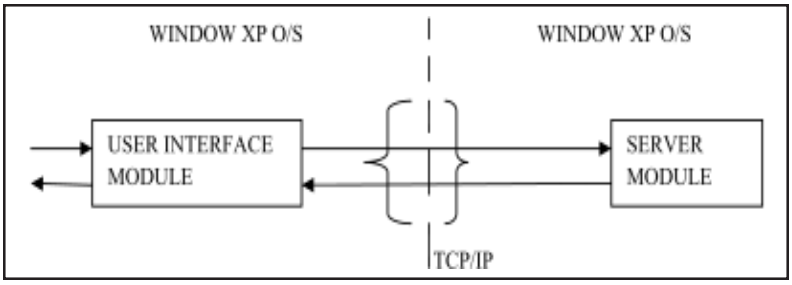

Figure 3. Modules of secure electronic payment system

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. This system includes two main parts: client module and server module. The purpose of this module is to pass request made by client to server. The server stores all transaction information in a set of data files. There are different types of clients that are customers and shops who own the shop owners. The communication between the client and server is TCP/IP protocol.

10.1 Requirements for e-payments:

- Atomicity :
  - – Money is not lost or created during a transfer
- Good atomicity
  - – Money and good are exchanged atomically
- Non-repudiation
  - – No party can deny its role in the transaction
  - – Digital signatures

The Below Figure is showing the process of Payment order system through the internet between the customer or bank.

11. Advantages of electronic payment system

The various factors that have leaded the financial institutions to make use of electronic payments are:

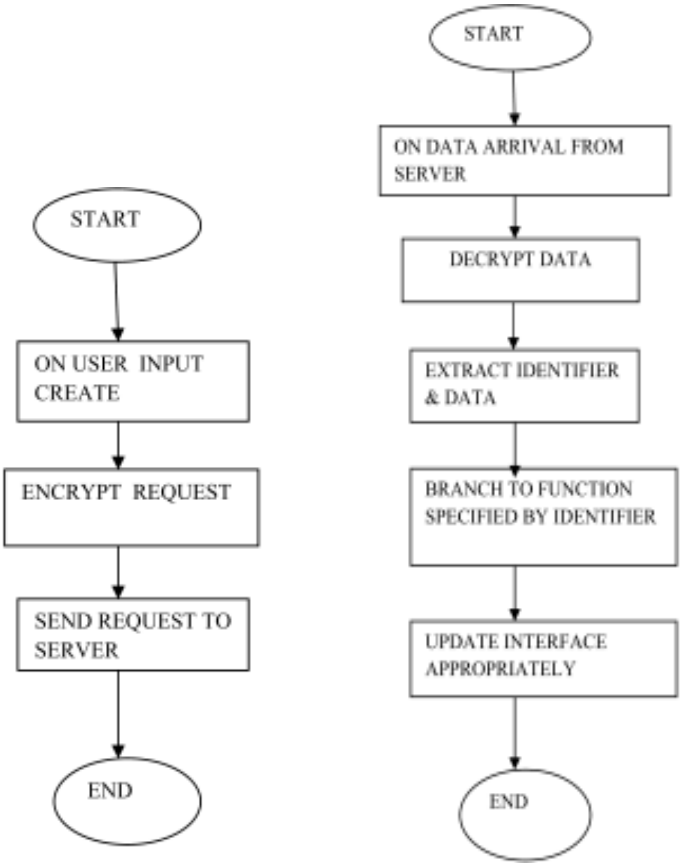

Figure 4. User interface Module Flow Chart

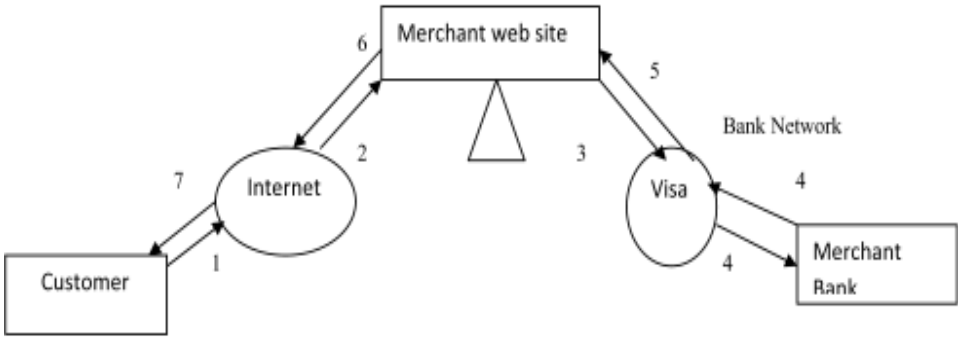

Figure 5. Processing of payment system

1. Decreasing technology cost:
The technology used in the networks is decreasing day by day, which is evident from the fact that computers are now dirt – cheap and internet is becoming free almost everywhere in the world.

2. Reduced operational and processing cost:
Due to reduced technology cost the processing cost of various commerce activities becomes very less. A very simple reason to prove this is the fact that in electronic transactions we save both paper and time.

3. Increasing online commerce: The above two factors have lead many institutions to go online and many others are following them.

11.1 Security Requirements

Except for the high level requirement that nobody wants to lose money, and everybody wants to be unobservable in their business to some extent, the concrete security requirements of electronic payment systems vary depending on their features and the trust assumptions put on their operation.

1. Integrity and Authentication

For a payment system, integrity means that no party loses money unless a payment is explicitly authorized by that party. Additionally a party might require to not receive any money without their explicit consent, e.g., in order to prevent unwanted bribery. Technically this is achieved by authenticating those messages that cause the transfer of money (withdrawal/payment/ deposit in cash-like systems, payment/clearing in cheque like systems). There are several possibilities how to do this:

- **Out-band Authorization:** The verifying party sends a notification to the authorizing party and requires that the authorising party approves or denies the authorisation offline, using a secure out-band channel (e.g., ordinary mail or phone calls).

- **Authorisation by passphrase:** The verifying party requires that messages from the authorising party include a cryptographic check value that is computed using a secret known to the authorising and verifying party only, e.g., a PIN or passphrase.

This achieves security against outsiders, but a dispute between authorising and verifying party about the origin of a well-authenticated message cannot be resolved (i.e., there is no non-repudiation of origin). This means that, e.g., a court would not be able to decide from the messages exchanged whether a disputed payment was authenticated by the buyer or by dishonest employees of the buyer's bank. Typically such insider fraud requires employee collusion since in PIN-based systems, customer PINs are usually well protected through encryption and tamper-resistant hardware at the bank. Additionally, short shared secrets like PINs of 4 or 6 digits cannot provide a high degree of security Therefore short shared secrets should only be used to control access to a physical token like a smartcard and this token should be used to do the actual authorization based on really secure cryptographic mechanisms.

- **Authorisation by signing:** The verifying party requires a digital signature of the authorising party. Digital signatures provide non-repudiation of origin: Only the owner of the secret signature key can sign messages (while everybody who knows the corresponding public verification key can test signatures). This enables to resolve disputes in case the authorising and verifying party disagrees about the authenticity of a message.

2. Confidentiality

Some or all parties involved may wish confidentiality of the transaction. Thereby the knowledge of the identity of buyer, seller, purchase content, amount, etc., are restricted to the participants involved, or even only to a subset of them (e.g., where anonymity or untraceability are desired).

3. Availability and Reliability

All parties are interested in being able to perform or receive payments whenever necessary. Payment transactions must be atomic, i.e., happen entirely or not at all, but never hang in an unknown or inconsistent state. No buyer would accept to lose money (or at least no significant amount) due to a network crash, or because the seller's server crashed. Availability and reliability presuppose that the underlying networking services and all software and hardware components are sufficiently dependable. Recovery from crash failures requires some sort of stable storage at all parties and specific resynchronization protocols.

4. Requirements for Mobile Trusted Hardware

To address the security requirements, digital signatures and secret key distribution functions are required, which makes it desirable that all parties involved have access to secure key storage. If payments are to be possible from any workstation, the secret key storage of a user must even be mobile, which in turn makes it necessary that users be provided with smart cards or similar secure devices.

4.1 SET (Secure electronic transaction) Protocol

Secure payment systems are critical to the success of E-commerce. There are four essential security requirements for safe electronic payments (Authentication, Encryption, Integrity and Non-repudiation). Encryption is the key security schemes adopted for electronic payment systems, which is used in protocols like SSL and SET. SET (Secure Electronic Transaction) is a

very comprehensive security protocol, which utilizes cryptography to provide confidentiality of information, ensure payment integrity, and enable identity authentication. For authentication purposes, cardholders, merchants, and acquirers will be issued digital certificates by their sponsoring organizations. It relies on cryptography and digital certificate to ensure message confidentiality and security.

Digital envelop is widely used in this protocol. Message data is encrypted using a randomly generated key that is further encrypted using the recipient's public key. This is referred to as the "digital envelope" of the message and is sent to the recipient with the encrypted message. The recipient decrypts the digital envelope using a private key and then uses the symmetric key to unlock the original message. Digital certificates, which are also called electronic credentials or digital IDs, are digital documents attesting to the binding of a public key to an individual or entity. Both cardholders and merchants must register with a certificate authority (CA) before they can engage in transactions. The cardholder thereby obtains electronic credentials to prove that he is trustworthy. The merchant similarly registers and obtains credentials. These credentials do not contain sensitive details such as credit card numbers. Later, when the customer wants to make purchases, he and the merchant exchange their credentials. If both parties are satisfied then they can proceed with the transaction.

11.3 Problem with SSL

The SSL protocol, widely deployed today on the Internet, has helped create a basic level of security sufficient for some hearty souls to begin conducting business over the Web. SSL is implemented in most major Web browsers used by consumers, as well as in merchant server software, which supports the seller's virtual storefront in cyberspace. Hundreds of millions of dollars are already changing hands when cybershoppers enter their credit card numbers on Web pages secured with SSL technology. In this sense, SSL provides a secure channel to between the consumer and the merchant for exchanging payment information. This means any data sent through this channel is encrypted, so that no one other than these two parties will be able to read it. What we want here is a protocol very similar to credit card transactions at a local store, something SSL doesn't mimic in functionality. The purpose of the SET protocol is to establish payment transactions that

- provide confidentiality of information;
- ensure the integrity of payment instructions for goods and services order data;
- Authenticate both the cardholder and the merchant.

12. Objectives Electronic Payment System

Their main expectation in the electronic payment system is that:

1. They can use the electronic payment system to attract more customers, sell more goods and services and get their payment on time
2. It have a low cost so easily can use.
3. Fast, easy to use, easy to set up

13. Conclusion

It is less expensive to have no online payment mechanism, but customer expectations have grown in recent years and you could be failing to capture your market and our choices will ultimately affect the success of our business. Electronic payment methods may be costly and challenging but they will give you the competitive and growing edge. This paper aims to explore the outlook of EPSs, based on a comprehensive review of current systems, their usage levels and the problems of application. This paper further believes that in the future, mobile payment systems and micro-payment systems providing significant convenience to individual customers will lead the way in the development of EPSs.

References

[1] E-commerce and mobile commerce technologies Dr.U.S. Pandey, Er. Saurabh shukla ,S.CHAND Publication.

[2] Singh, Sumanjeet (2009). EMERGENCE OF PAYMENT SYSTEMS IN THE AGE OF ELECTRONIC COMMERCE: THE STATE OF ART. *Global Journal of International Business Research* 2 (2) 7

[3] Electronic Payment Systems, Janson, P., (ZRL), Waidner, M. (ZRL) (1996). Final *SEMPER* Activity Paper 211ZR017 Vers. 7.

[4] Secure Electronic Transaction (SET protocol) Yang Li & Yun Wang.

[5] http://www.allfreeessays.com/topics/types-of-electronic-payment-systems

[6] www.cis.upenn.edu/~lee/00emtm553/e-payment.ppt

[7] http://www1.american.edu/initeb/sm4801a/epayment3.htm

[8] http://www.electronic-payments.co.uk/online_payments.jsp

[9] World Academy of Science, Engineering and Technology. (2008). Design and Implementation of Secure Electronic Payment System (Client) Pyae Pyae Hun.

[10] http://knol.google.com/k/electronic-payment-systems