Chapter 3

"It was the destiny of money to become digital"

-OECD

ELECTRONIC PAYMENT AND SECURITY SYSTEMS

Electronic Payment System

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. Section I aims to study the framework of electronic payment system. This section discusses the concept of electronic payment system and describes the different types of electronics payment systems. Further, a comparison has been made between different electronic payment systems. In the end of section, concluding remarks are given.

As payment[1] is an integral part of mercantile process, electronic payment system is an integral part of e-commerce. The emergence of e-commerce has created new financial needs that in many cases cannot be effectively fulfilled by traditional payment systems. For instance, new types of purchasing relationships-such as auction between individuals online-have resulted in the need for peer-to-peer[2] payment methods that allows individuals to e-mail payments to the other individual. Recognizing this, virtually all interested parties (i.e. academicians, government, business community and financial service providers) are exploring various types of electronic payment system and issues surrounding electronic payment system and digital currency. Some proposed electronic payment systems are simply electronic version of existing payment systems such as checks and credit cards, while, others are based on the digital currency technology and have the potential for definitive impact on today's financial and monetary system. While popular developers of electronic payment system predict fundamental changes in the financial sector because of the innovations in electronic payment system (Kalakota & Ravi, 1996)[3]. Therefore, electronic payment systems and in particular, methods of payment being developed to support electronic commerce cannot be studied in an isolation. A failure to take place these developments into the proper context is likely to result in undue focus on the various experimental initiatives to develop electronic forms of payment without a proper reflection on the broader implications for the existing payment system.

---

[1] Payment represents both cash and non-cash financial transactions, which take place between two or more parties. But, in a strict sense of word 'payment' represents only non-financial transaction. It is more common for two parties exchanging value to hold accounts with alternative banks, in which both banks become the parties of payment.

[2] Peer-to-peer refers to the design of a service that does not rely on centralized networking services such as D.N.S. (Domain Name System-a unique name of collections of computers connected to networks such as Internet) to connect and users' computers and accounts for the unpredictable accessibility of these end nodes in making connections between the users. Participants in the peer-to-peer network, whether individual or companies, exchange information directly with one another, bypassing central exchanges. In short, peer-to-peer is more of a bazaar what customers will find until he/she get there. (Erikson, J. (2003), *Dictionary of E-Commerce*, New Delhi: Anmol Publications Pvt. Ltd., p.151.

[3] Kalakota, Ravi and Whinston, B. Andrew (1996), *Frontiers of Electronic Commerce*, Singapore: Pearson Education, p. 295.

Concept of Electronic Payment System

Payment systems that use electronic distribution networks constitute a frequent practice in the banking and business sector since 1960s[4], especially for the transfer of big amounts of money. In the four decades that have passed since their appearance, important technological developments[5] have taken place, which on the one hand have expanded the possibilities of electronic payment systems and on the other hand they have created new business and social practice, which make the use of these systems necessary. These changes, naturally, have affected the definition of electronic payments[6], which is evolving depending on the needs of each period. In its, most general form, *the term electronic payment includes any payment to businesses, bank or public services from citizens or businesses, which are executed through a telecommunications or electronic networks using modern technology.* It is obvious that based on this definition, the electronic payments that will be the objects of present result, are the payment that are executed by the payer himself, whether the latter is a consumer or a business, without the intervention of the another natural person. Furthermore, the payment is made from distance, without the physical presence of the payer and naturally it does not include cash. By providing such definition for the electronic payment system, researcher include the transfer of information concerning the accounts of the parties involved in the e-commerce transactions, as well as the technological means of distribution channels through which the transactions is executed.

Size of Electronic Payments

Electronic payment system is conducted in different e-commerce categories such as Business-to-Business (B2B), Business-to-Consumer (B2C), Consumer-to-Business (C2B) and Consumer-to-Consumer (C2C). Each of which has special characteristics that

---

[4] BankAmerica, in Fresno, California, executes the first mass mailing of credit cards in (1960); Westminister Bank installs first automated teller machine (ATM) at Victoria, London Branch in 1967.

[5] In the year, 1967, the New York Clearing House launched CHIPS (Clearing House Interbank Payment System) which provides US Dollar funds –transfer and transactions settlements online and in real time. In the late 1970s, Chemical Bank launched its Pronto system providing 3,000 computer terminals to customers' home linked to its central computers by telephone. It offers a range of facilities: balance inquiries, money transfer between Chemical Bank accounts, and bill payments to selected local stores. The stumbling blocks for the first generation home building system in general was who is to pay for terminals at home. In the year 1985, EDI (Electronic Data Interchange) extensively used in bank-to-bank payment systems. In 1994, digital cash trails by DigiCash of Holland conducted online. And in the year 1995, Mondex electronic currency trails begin in Swindon, England.

[6] A real revolution in the meaning of electronic payment system came with the development of EFT (Electronic Fund Transfer) technology. EFT is a technology (one of the electronic commerce technologies) that allows the transfer of funds from the bank account of the one person or organization to that another. EFT is also used to refer to the action of using this technology. It is an important addition in organization that implements EDI in their organization. Consequently, the online remittance of funds appeared to be the next logical step in a progressive move towards the electronic funds transfer and banking, a process that had begun long before the Internet itself. There is, however, a crucial distinction between the pre-Internet electronic fund transfer system and the online payment system being used and developed in the conjunction with e-commerce. The former took place almost exclusively over proprietary networks, which the latter occur over a publicly accessible electronic medium. Charkrabarthi, Rajesh et al (2002), *The Asian Manager's Handbook of E-Commerce,* New Delhi: Tata McGraw Hill.)

depend on the value of order. Danial, (2002)[7] classified electronic payment systems as follows:

- *Micro Payment (less than $ 10) that is mainly conducted in C2C and B2C e-commerce.*
- *Consumer Payment that has a value between $ 10 and $ 500. It is conducted mainly in B2C transactions.*
- *Business Payment that has the value more than $ 500. it is conducted mainly in B2B e-commerce .*

B2B transactions account about 95% of e-commerce transactions, while others account about 5% (Turban *et al,* 2004)[8]. P2P, which is related to the C2C category transactions, is relatively small due to its stiff usability.

Further, Cavarretta and de Silva (1995)[9], identify three classes of typical electronic transactions:

- *Tiny value transactions: below $1.*
- *Medium value transactions: between $ 1 and $ 1,000*
- *Large value transactions: above $ 1,000.*

Systems that can support tiny value transactions have to trade-off between conveniences of transactions (the major part of a cost in an extremely cheap transaction) vs. the security or durability of transactions. On the other side of the amount range, large value transactions will require highly secure protocols whose implementations are costly: be on-line and/or carry traceability information. Finally, nearly all the system can perform medium value transactions.

Conventional vs. Electronic Payment System

To get into the depth of electronic payment process, it is better to understand the processing of conventional or traditional payment system. A conventional process of payment and settlement involves a buyer-to-seller transfer of cash or payment information (i.e., cheque and credit cards). The actual settlement of payment takes place in the financial processing network. A cash payment requires a buyer's withdrawals form his/her bank account, a transfer of cash to the seller, and the seller's deposit of payment to his/her account. Non-cash payment[10] mechanisms are settled by adjusting i.e. crediting and debiting the appropriate accounts between banks based on payment information conveyed via cheque or credit cards.

---

[7] Danial, Amor (2002), *E-Business (R) evolution,* New York: Prentice Hall.

[8] Turban, E.; King, D. and D. Viehland (2004), *Electronic Commerce: A Managerial Perspective*: Prearson Education.

[9] Cavarretta, F. and de Silva, J. (1995), "*Market Overview of the Payments Mechanisms for the Internet Commerce*", accessed on http://www.mba96.hbs.edu/fcavarretta/money.html.

[10] Non-cash payment requires three separate elements. The buyer must have an agreed means of payment authorization and instructuring its bank to affect a transfer of funds. The seller's bank and buyer's bank need an agreed method of exchange payment instructions. This is referred to as payment clearing.

Figure 3.1: Conventional/Traditional Payment System

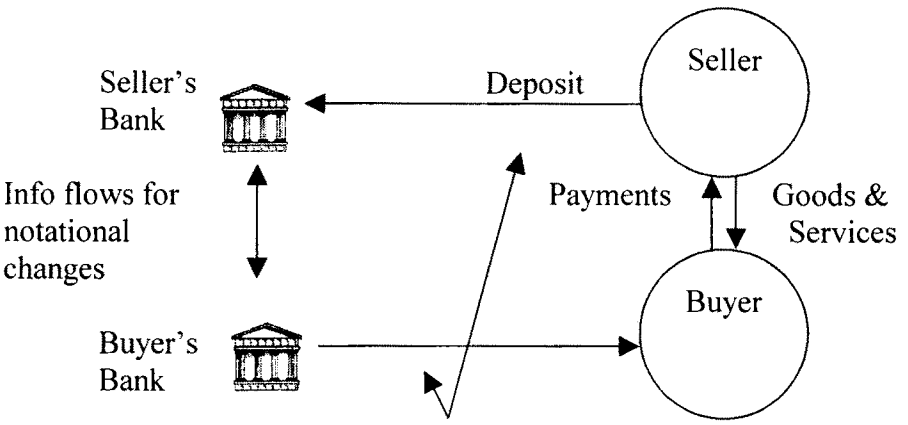


Figure 3.1 is simplified diagram for both cash and non-cash transactions. Cash moves from the buyers' bank to sellers' bank through face-to-face exchange in the market. If a buyer uses a non-cash method of payment, payment information instead of cash flows from the buyer to the seller, and ultimate payments are settled between affected banks, who notationally adjust accounts based on payment information[11].

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[12]. 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[13]. 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[14]. The nature of digital currency or

---

[11] In real markets, this clearing process involves some type of intermediaries such as credit card services or cheque processing clearing companies. Schematically most payment systems are based on similar process.

[12] Bhatia, Varinder (2000), *E-Commerce (Includes E-Business)*, New Delhi: Khanna Book Publishing Co.

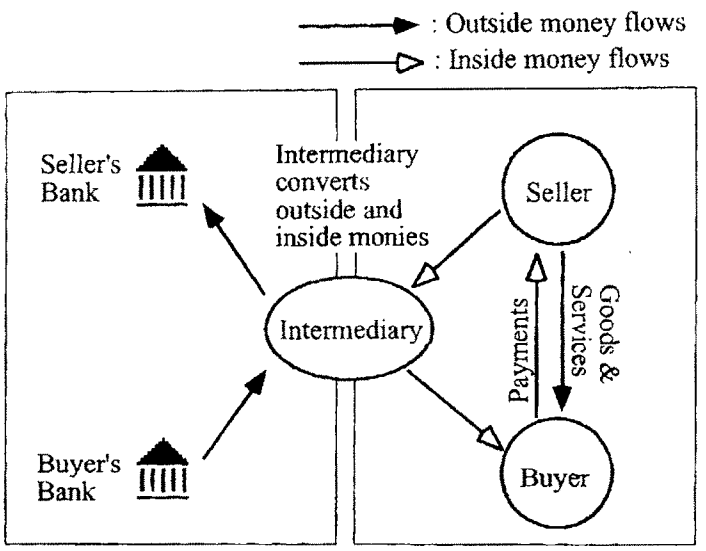
[13] In this case, intermediary acts as a centralized commerce enabler maintaining membership and payment information for both sellers and buyers. A buyer need only send the seller his identification number assigned by the intermediary.

[14] Development in cryptography (science of disguising message to only the writer and the intended receivers are able to read them) has brought a new kind of money: the digital currency (e.g. DigiCash System {Chaum, (1992)}, the CAFÉ Project {Boly *et al.*, (1994)} and Mondex. The digital currency, encoded strings of digits, can be carried on a smart card or stored on a computer disk. Like a travelers' checque, a digital coin is a floating claim on a bank or other financial institution that is not linked to any particular account. Chaum, D. (1992), *"Achieving Electronic Privacy"*, Scientific American, August,pp 96-101 accessed on http://www.digicash.support.nl/publish/sciam.html.

Boly, J. P. et al., (1994), *" The ESPRIT Project CAFÉ-High Security Digital Payment System"*, ESORICS 94, Third European Symposium on Research in Computer Security, Brighton, LNCS 875,

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 (i.e. EFT based and intermediary based) 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. Figure 3.2 shows digital currency based payment system.

Figure 3.2: Electronic Payment System



In this figure, it is shown that intermediary acts as an electronic bank, which converts outside money (e.g. Rupees or US $), 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[15] on money and monetary system with implications extending far beyond more transactional efficiency.

Types of Electronic Payment Systems

With the growing complexities in the e-commerce transactions, different electronic payment systems have appeared in the last few years. At least dozens of electronic payment systems proposed or already in practice are found[16]. The grouping can

---

Spring- Verlage, Berlin, pp 217-230. accessed on http://www.zurich.ibm.ch/technology/Security/Sirene/Publ/ BBCM1_94cafeEsorics.ps.gz.

[15] Already digital currency has spawned many types of new businesses: software vendors for currency server system; hardware vendor for the smart cards readers and other interface devices; technology firms for security, encryption and authentication and new banking services interfacing accounts in digital currency and conventional currency.

[16] Murthy, C.S.V. (2002), *E-Commerce: Concepts, Models and Strategies*, New Delhi: Himalaya Publishing House, p. 626.

be made on the basis of what information is being transferred online[17]. Murthy (2002) explained six types of electronic payment systems: (1) PC-Banking (2) Credit Cards (3) Electronic Cheques (i-cheques) (4) Micro payment (5) Smart Cards and (6) E-Cash. Kalakota and Whinston (1996) identified three types of electronic payment systems: (1) Digital Token based electronic payment systems[18], (2) Smart Card based electronic payment system[19] and (3) Credit based electronic payment systems[20]. Dennis (2001)[21] classified electronic payment system into two categories: (1) Electronic Cash and (2) Electronic Debit-Credit Card Systems. Thus, electronic payment system can be broadly divided into four general types[22]:

- *Online Credit Card Payment System*
- *Electronic Cheque System*
- *Electronic Cash System and*
- *Smart Card based Electronic Payment System*

Online Credit Card Payment System: It seeks to extend the functionality of existing credit cards[23] 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[24]. This form of payment system has several advantages, which were never available through the traditional modes of payment. 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

---

[17] Kalakota, Ravi and Whinston, B. Andrew (1996), *Frontiers of Electronic Commerce*, New Delhi: Pearsons Publication.

[18] It includes: (1) Electronic Tokens, Electronic Cash and Electronic Cheques.

[19] It includes: (1) Relationship based Smarts Cards (2) Electronic Purses and Debit Cards and Smart Cards Readers and Smart Phones.

[20] It includes: Encryption and Credit Cards and third party processors and Credit Cards.

[21] Dennis, Abrazhevich (2001), *"Classifications and Characteristics of Electronic Payment Systems"*, Lecture Notes in Computer Science, Vol. 21, No. 5, pp. 81-90.

[22] Anderson, M.M. (1998), *"Electronic Cheque Architecture, Version 1.0.2"*, Financial Services Technology Consortium, September

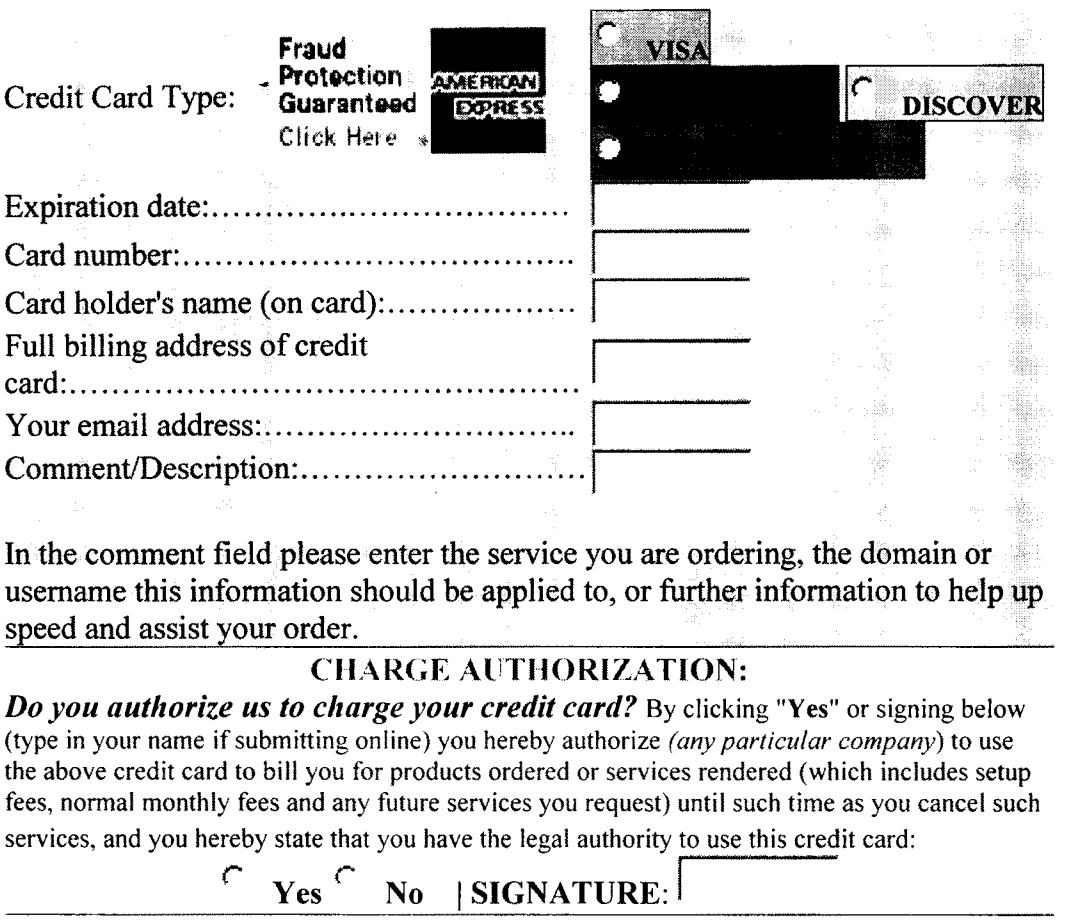
[23] Credit card is made of plastic whose holder has been granted a revolving credit lines. This enables the holder to make purchase and/ or cash advances upto a pre arranged limits. The credit granted can be settled in full by the end of a specific period or in part, with the balance taken as extended credit. Interest may be charged on the transaction amounts from the date of each transaction or only the extended credit where the credit granted has not been settled in full. (http://www.rba,gov.in/Glosssary/text_only.asp). The card normally contains the cardholders name and account number and many other information encoded on the magnetic strip. Some credit cards may be used in ATM (http://www.treas.gov/glossar/gloss-c.htm). Credit cards began in the late 40's when banks began giving out paper certificates that could be used like cash in local stores. Frankline National Bank of New York used the first real credit card in 1951.

[24] Laudon, C. Kenneth and Traver, Carol (2002), *E-Commerce*, New Delhi: Pearson Education.

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. This can be understood very easily with the format (Figure 3.3) of Credit Card Payment Form.

Figure 3.3: Credit Card Payment Form



Kalakota Whinston (1996)[25], break credit card payment on online networks into three basic categories: (1) payment using clean credit card details (2) payment using encrypted credit card details and (3) payment using third party verification.

[25] Kalakota, Ravi and Whinston, B. Andrew (1996), Frontiers of Electronic Commerce, New Delhi: Pearson Education.

Electronic Cheque Payment System: Electronic cheques[26] address the electronic needs of millions of businesses, which today exchange traditional paper cheques with the other vendors, consumers and government. The e-cheque method[27] was 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 uncoded 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. Electronic cheque system has many advantages: (1) they do not require consumers to reveal account information to other individuals when setting an auction (2) they do not require consumers to continually send sensitive financial information over the web (3) they are less expensive than credit cards and (4) they are much faster than paper based traditional cheque[28]. But, this system of payment also has several disadvantages. The disadvantage of electronic cheque system includes their relatively high fixed costs, their limited use only in virtual world and the fact that they can protect the users' anonymity. Therefore, it is not very suitable for the retail transactions by consumers, although useful for the government and B2B operations because the latter transactions do not require anonymity, and the amount of transactions is generally large enough to cover fixed processing cost. The process[29] of electronic chequing system can be described using (figure 3.4) 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 vendor's account and a credit advice is sent to him.

---

[26] 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.

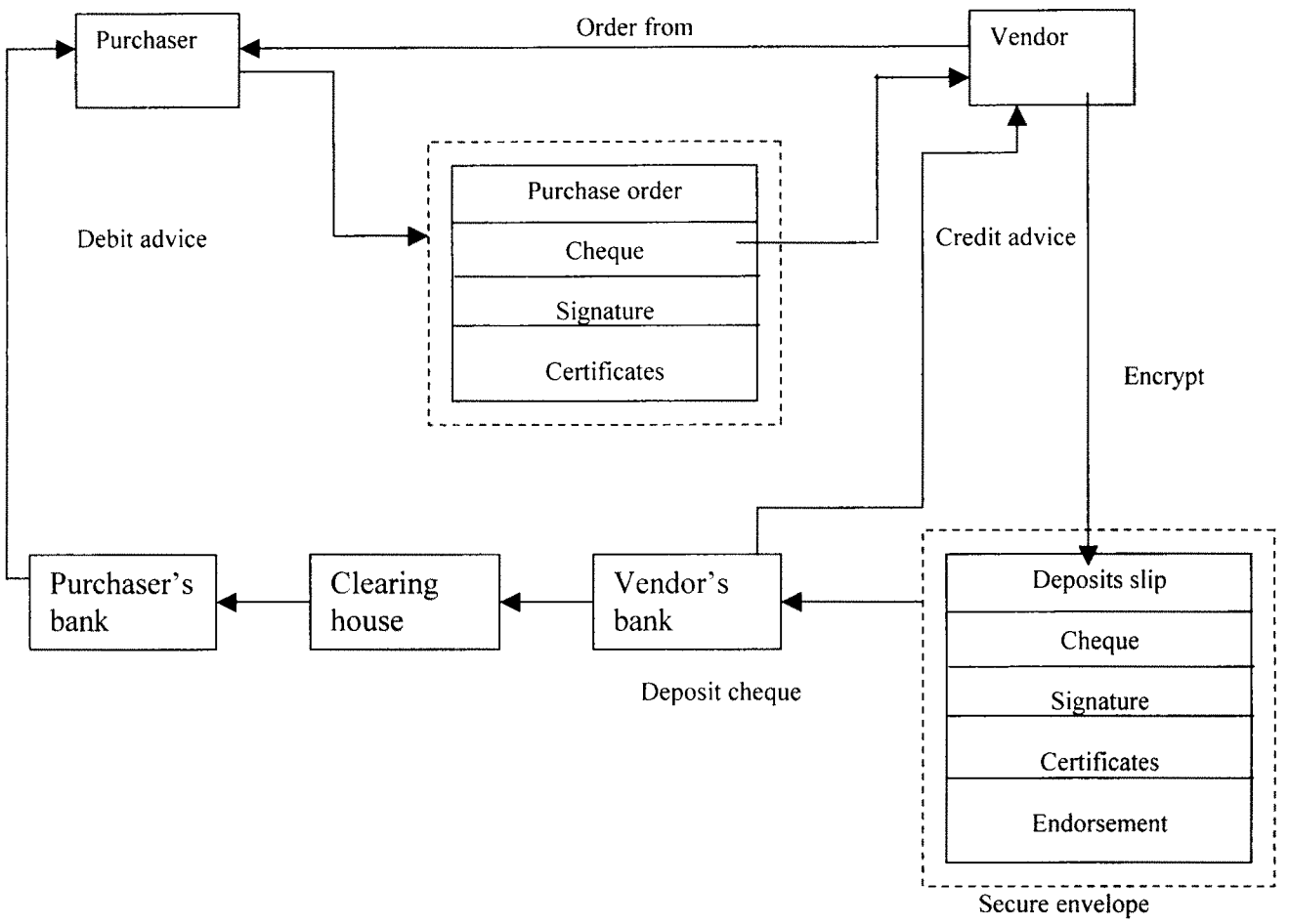
[27] Electronic cheque is different from the electronic fund transfer (EFT) in several ways. For electronic chequing, electronic versions of cheques are issued, received and processed. So, the payee issues an electronic cheque for each payment. For EFT, automatic withdrawals are made for monthly bills or other fixed payments; no charges are issues.

[28] [28] Laudon, C. Kenneith and Traver, Carol (2002), *E-Commerce*, New Delhi: Pearson Education.

[29] Thus, a complete electronic cheque transaction may consist of several basic steps and these steps are executed in three distinct and optionally separate phases. In the first phase, the consumer makes a purchase; in the second phase, the merchant sends the electronic cheques to its bank for the redemption. In the third phase, the merchant's bank approaches the clearinghouse or consumer's bank to cash the electronic cheques. (Diwan, Parag and Sharma, Sunil (2001), *E-Commerce: A Managerial's Guide to E-Business*, New Delhi: Excel Books.

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

Figure 3.4: Clearing cheque payment electronically



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.

Electronic Cash Payment System: Electronic cash (e-cash)[30] 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[31]. 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. E-cash presents some characteristics like monetary value[32], storability and

[30] 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.

[31] Kalakota and Whinston (1996)

[32] e-cash must have monetary value; it must be backed by either cash (currency),. Bank authorized credit, or a bank's certified cashier cheque.

irretrievability[33], interoperability[34] and security[35]. All these characteristics make it more attractive payment system over the Internet. Added to these,, this payment system offers numerous advantages like authority, privacy[36], good acceptability, low transactions cost, convenience and good anonymity[37]. But, this system of payment also has many limitations like poor mobility[38], poor transaction efficiency[39] and high financial risk, as people are solely responsible for the lost or stolen. Gary and Perry (2002), just like real world currency counterpart, electronic cash is susceptible to forgery. It is possible, though increasingly difficult, to create and spend forged e-cash.

E-Cash Structure: e-cash structure could be identified as a string of bits that represents certain values such as reference number and digital signature, which could be used for the security purpose to prevent forgery and criminal use (Wright, 2002)[40]. But, the structure proposed by Wright (2002) needs some extension to make e-cash more secure. Therefore, the present model (Figure 3.5) adds a digital watermark to e-cash structure to protect it from the illegal copy and forgery activities further, the model modified the structure of the reference number to support tractability as shown in the figure 3.5.

Figure 3.5: E-Cash Structure

Currency[41]	**Value**[42]	**Reference**[43]	**Digital Signature**[44]	**Digital Watermark**[45]

The proposed e-cash structure is comparatively better than suggested by Wright (2002), because security issue is given importance of top most priority in the present

[33] E-cash must be storable and retrievable. Remote storage and retrieval (e.g., from a telephone or personal communication device) would allow users to exchange e-cash from home, office or while traveling. The cash could be stored on a remote computer's memory in smart cards, or in other easily transported standard or special purpose devices.

[34] It must be interoperable-that is, exchangeable as payment for other e-cash, paper cash; goods or services, lines of credit, deposits in banking accounts, bank notes or obligations etc.

[35] E-cash should not be easy to copy or tamper with during exchange; this includes preventing and detecting duplication and double spending.

[36] The store or third parties online have no way of attaining the consumer's bank account information.

[37] Companies have no way of finding out the consumer's account information, and the distributors of e-cash have no way of finding out how e-consumers spend the e-cash.

[38] Consumers can only use computers that have the e-cash purse system.

[39] Needs to enter a large database to make comparison.

[40] Wright, David (2002), *Comparative Evaluation of Electronic Payment System,* INFO 2002.

[41] Currency that defines the issued currency to sport multi currencies e-cash.

[42] Value that determines the value of e-cash.

[43] Reference number that allows the issuer or any other authorized party to trace e-cash movement. It has the following four sub types

a. Issuer part, which is used as a reference to the issuer.
b. Client part, which is used as a reference to the customer who orders the e-cash for the first time.
c. Owner part, which is used to represent the ID of the new owner of the e-cash each time.
d. Final part, which is used to check the generated digit each time.

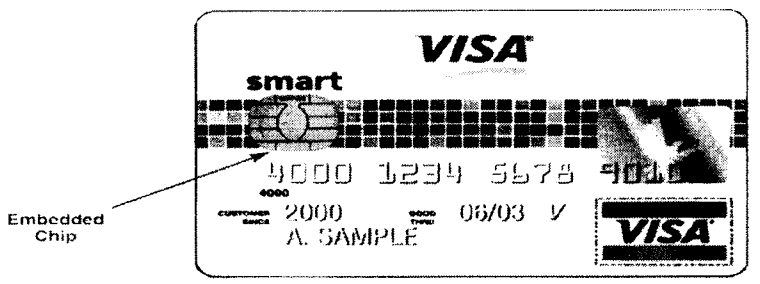
[44] Digital signature is used to authenticate the identity of the issuer as an authorized party.

[45] Digital watermark is used for copyright protection. It inserts invisible data into the digital file. In the present model, e-cash structure uses the digital watermark to prevent forgery or illegal copy of the e-cash.

model. But, still there are certain concerns to be addressed for an electronic cash system[46]. For example, who has the right to issue electronic cash? Can every bank issue its own money? If so how do you prevent fraud? And who will monitor the banking operations to protect consumers?[47] Many of these concepts relate to the legal and banking regulatory aspects. However all these issues are beyond the scope of the study and therefore, cannot be included here. But, these issues must be addressed before establishing a complete e-cash based payment system.

Smart Cards based Electronic Payment System: 'Smart cards' are receiving renewed attention as a mode of online payment. 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[48] with inbuilt transaction processing capability[49].

Figure.3. 6: Smart Card Image



This card also contains some kinds of an encrypted key that is compared to a secret key contained on the user's processor. Some smart cards have provision to allow users to enter a personal identification number (PIN) code. Smart cards have been in use for well over the two decades now and have been widespread mostly in Europe and Asian Countries. Owing to their considerable flexibility, they have been used for a wide range of functions like highway toll payment, as prepaid telephone cards and as stored value debit cards. However, with the recent emergence of e-commerce, these devices are increasingly being viewed as a particularly appropriate method to execute online payment system with considerably greater level of security than credit cards.

---

[46] Processing of electronic payment system: a consumer first had to establish an account at a bank that was using e-cash system. Once the account is established, the consumer then downloaded the e-wallet software onto his/her computer's hard drive. Then consumer could request a transfer of digital cash. Once the digital wallet had cash, the consumer could spend that cash at merchants who were willing to accept it. The software would deduct the cash from digital wallet and transfer it to the merchant. The merchant could then transfer the cash back to the bank to confirm that it had not been double spent. The bank would cancel the e-coins or credit the merchant account at bank.

[47] Diwan, Parag and Sharma, Sunil (2000), *E-Commerce: A Manager's Guide to E- Business,* New Delhi: Excel Books.

[48] Credit cards store a single charge account number in the magnetic strip on the back, smart cards can hold 100 times more data, including multiple credit card numbers and information regarding health insurance, transportation, personal identification, bank accounts and loyalty programs, such as frequent flyer accounts. This capacity makes them attractive alternatives to carrying a dozen or so credit and ID cards in a physical wallet.

[49] Chakrabarti, Rajesh and Kardile, Vikas (2002), *E-Commerce: The Asian Manager's Handbook,* New Delhi: Tata McGraw Hill.

Compared with traditional electronic cash system, smart cards based electronic payment systems do not need to maintain a large real time database. They also have advantages, such as anonymity, transfer payment between individual parties, and low transactional handling cost of files. Smart cards are also better protected from misuse[50] than, say conventional credit cards, because the smart card information is encrypted. Currently, the two smart cards based electronic payment system- Mondex[51] and Visa Cash are incompatible in the smart cards and card reader specification. Not knowing which smart card system will become market leader; banks around the world are unwilling to adopt either system, let alone other smart card system. Therefore, establishing a standard smart card system, or making different system interoperable with one another is critical success factors for smart card based payment system.

Kalakota and Whinston (1996), classified smart cards based electronic payment system as (1) relationship based smart cards and electronic purses. Electronic purses, which may replace money, are also known as debit card[52]. Further Diwan and Singh (2000)[53] and Sharma and Diwan (2000)[54], classified[55] smart cards into four categories. These are: (1) memory cards: this card can be used to store password or pin number. Many telephone cards use these memory cards (2) shared key cards: it can store a private key such as those used in the public key cryptosystems. In this way, the user can plug in the card to a workstation and workstation can read the private key for encryption or decryption (3) signature carrying card: this card contains a set of pregenerated random numbers. These numbers can be used to generate electronic cash (4) signature carrying cards: these cards carry a co-processor that can be used to generate large random numbers. These random numbers can then be used for the assignment as serial numbers for the electronic cash.

---

[50] For example conventional credit cards clearly show your account number on the face of the card. The card number along with a forged signature is all that a thief needs to purchase items and charge them against your card. With smart card, credit theft is practically impossible because a key to unlock the encrypted information is required, and there is no external number that a thief can identify and no physicals signature that a thief can forge. In addition, smart cards provide the advantages of portability and convenience.

[51] Multifunctionary is one of the most exceptional features of the Mondex, a system that intends become "an *electronic equivalent of cash*". It is based on a smart card that can hold money and transfer it in both ways. The Mondex card is a debit card in the sense that can only be used to spend as long as it holds previously loaded money. The Mondex technology, in the development since 1990s, is exclusively runs by Mondex International, a London based firms in which Master cards holds 51% of share since the end of 1996.

[52] Wallet sized smart cards embedded with programmable microchips that store sums of money for people to use instead of cash for everything from buying food, to making photocopies, to paying subways fares. The electronic purse works in the following manners. After the purse is loaded with money, at an ATM or through the use of an inexpensive special telephone, it can be used to pay for, say, candy in a vending machine equipped with the card reader. The vending machine needs only to verify that a card is authentic and there is enough money available for the chocolate bar. In one second, the value of purchase is deducted from the balance on the card and added to e-cash box in the vending machine. The remaining balance on the card is displayed by the vending machine or can be checked at an ATM or with a balance ready device.

[53] Diwan, Parag and Singh, Dharmvir (2000), *Computer Networks Driven E-Commerce Technologies*, New Delhi: Amexcel Publisher Pvt. Ltd.

[54] Sharma, Sunil and Diwan Parag (2000), *E-Commerce: A Manager's Guide to E-Business*, New Delhi: Excel Books.

[55] Broadly these classifications are based on the technologies used in the smart cards based payment system.

Comparison of Electronic Payment Systems

The electronic payment system- the ability to pay electronically for goods and services purchased online- are an integral part of e-commerce and an essential infrastructure for e-commerce models. One of the major reasons for the widespread of e-commerce transactions is perhaps the rapid development and growth of various electronic payment systems. In the developed countries, credit cards have been used even before the advent of Internet. The present part of the study revealed many electronic payment systems and broadly these electronic payment system can be grouped or classified into four categories: (1) Online Credit Card Payment System (2) Online Electronic Cash System (3) Electronic Cheque System and (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. Figure 3.7 presents the comparison of various electronic payment systems.

Figure 3.7: Comparison of electronic payment systems

Features	Online Credit Card Payment	Electronic Cash	Electronic Cheque	Smart Cards
Actual Payment Time	Paid later	Prepaid	Paid later	Prepaid
Transaction information transfer	The store and bank checks the status of the credit card	Free transfer. No need to leave the name of parties involved	Electronic checks or payment indication must be endorsed	The smart card of both parties make the transfer
Online and offline transactions	Online transactions	Online transactions	Offline transfers are allowed	Offline transfers are allowed
Bank account involvement	Credit card account makes the payment	No involvement	The bank account makes the payment	The smart card account makes the payment
Users	Any legitimate credit card users	Anyone	Anyone with a bank account	Anyone with a bank or credit card account
Party to which payment is made out	Distributing Bank	Store	Store	Store
Consumer's transaction risk	Most of the risk is borne by the distributing bank, consumers only have to bear part of the risk	Consumer is at risk of the electronic cash getting stolen, lost, or misused	Consumer bears most of the risk, but the consumer can stop check payments at any time	Consumer is at risk of the smart card getting stolen, lost or misused

Current degree of popularity	Credit card organizations check for certification then total the purchases. Therefore, it can be used internationally, and is the most popular payment type	Unable to meet financial internet standards in the areas of expansion potential and internationalism.	Can not meet international standards, therefore its not very popular	Credit card organizations check for certification then total the purchases. Therefore it can be used internationally, and is becoming more widely used.
Anonymity	Partially or entirely anonymous	Entirely anonymous	No anonymity	Entirely anonymous, but if needed, the central processing agency can ask stores to provide information about a consumer
Small payments	Transaction costs are high. Not suitable for small payments	Transaction costs are low, suitable for small payments	Allows stores to accumulate debts until it reaches a limit before paying for it. Suitable for small payments	Transaction costs are low. Allows stores to accumulate debts until it reaches a limit before paying for it. Therefore, it is suitable for small payments
Database safeguarding	Safeguards regular credit card account information	Needs to safeguard a large database, and maintain records of the serial numbers of used electronic cash.	Safeguards regular account information	Safeguards regular account information
Transaction information face value	Can be signed and issued freely in compliance with the limit	Face value is often set, and cannot be changed	Can be signed and issued freely in compliance with the limit	Can be deducted freely in compliance with the limit
Real/Virtual world	Can be partially used in real world	Can only be used in the virtual world	Limited to virtual world, but can share a checking account in the real world.	Can be used in real or virtual worlds.
Limit on transfer	Depends on the limit of the credit card	Depends on how much is prepaid	No limit	Depends on how much money is saved.
Mobility	Yes	No	No	Yes

After analysis and comparison of various modes of electronic payment systems, researcher comes to the following conclusions:

Concluding Remarks:

- Credit card is the most popular methods of payment over Internet. Internet buyers seem to prefer credit cards to other electronic payment system that have been made available to them. One reason may be the simple familiarity with the credit card, as it is the oldest form of electronic payment system. E-commerce is still new and intimidating to many. It is easier for the buyers to make purchase on the Internet when they can use the familiar payment method, like credit card. However, this payment system suffered from many limitations like security[56], merchant risk[57], high costs[58] and affordability[59]. For sellers' side, credit card has strategic disadvantages like: (1) credit cards are subject to percentage fees and these charges erode the profits margin, particularly on the inexpensive goods and services; (2) a buyers who uses a credit card may refuse to pay the issuer on the grounds that he/she has a claim or defense arising out of the underlying transactions. When this happens, the issuer may pass the loss back to the seller. Above all, credit cards have highest possibilities of frauds. Therefore, both buyers and sellers are shifting from credit cards to other innovative payment products, such as smart cards and electronic money. But, still it is expected that the buyers may continue to prefer credit card system, particularly when making expensive purchase.
- It is quite difficult, if not impossible, to suggest that which payment system is best. Some systems are quite similar, and differ only in some minor details. Further, all these systems have ability or potential to displace cash. Added to this, widely different technical specifications makes it difficult to choose an appropriate payment system. On the basis of above analysis it is concluded that, smart cards based electronic payment system is best. It has numerous advantages over the other electronic payment systems. It is expected that in the future smart cards will eventually replace the other electronic payment systems. Therefore, establishing a standard smart card based system, or making different system interoperable with one another is critical success factor for the smart cards based payment system. Smart card organizations around the world must establish a smart card interface standard and a conformance testing organization to make all smart card system compatible; otherwise smart card related products will not develop fully.
- Monetary value, convenience, authorization, security, authentication, non-refutability, accessibility and reliability and anonymity are the most desirable properties of any electronic payment system. Functionally, money technologies

---

[56] Neither the merchant nor the consumer is authenticated. The existing system offers very poor security. The merchant could be a criminal organization designed to collect credit cards numbers, and the consumers could be using stolen or fraudulent cards.

[57] The risk facing merchant is high- consumers can repudiate charges even through the goods have been shipped or the product downloaded.

[58] Costs for merchants are also very significant- roughly 3.5 % of the purchase plus a transaction fees of 20 to 30 % per transactions, plus other set up costs. The high costs make it undesirable to sell on the web for less than $ 10 (Laudon and Traver, 2002)

[59] Not everyone has the access to credit cards. Millions of people between the ages of 10 to 25 do not have the capacity to have credit cards. Even in America about 70 to 100 million adult cannot afford credit cards because of low incomes.

also need to achieve these operating characteristics: privacy, reliability, scalability[60], ease of use, personalize-able, seamlessness[61], interoperability[62], and cost effectiveness.

- It is also observed that different countries prefer the different forms of electronic payment system. Credits cards are dominant form of online payment system in the United States[63] (US); this is not true in other parts of the world. Only 50 % of consumers outside the US use credit cards for online purchase (Landon and Traver, 2002). In Europe (especially in UK) and other countries of developed world like Canada, New Zealand, and in some of the Asian Developing Countries like China. Thailand, Japan and Singapore, smart cards based electronic payment system is popular. Most of the developing countries like India rely much more on electronic funds transfer and smart cards based electronic payment system. Very few percent of people have credit cards and use of e-cheque is in vogue. Poor countries still rely on traditional cash and cheque system; they are not very much familiar with the electronic payment system because of poor infrastructure, poor economic conditions, lack of education etc. Outside the US, electronic payment system is heavily influenced by the host country's financial infrastructure (Lawarence, 2000)[64]. Added to these, legal regimes, IT Infrastructure, economic and social conditions, are the strong determinants of the methods of online payment and all these vary from country to country and even within the country.

[60] Ability to raise capacity over time. Technologies can be brought forward and replicate transactions thousands or millions of times, as necessary.

[61] Front grounds user interface operates with no impact from any vagaries of background infrastructure.

[62] Distinct hardware/software infrastructures can communicate and exchange data; if they were identical.

[63] This fact can be supported by the Research Conducted by Jupiter Media Matrix (2000). The research revealed that credits cards are the most dominant methods of online payment in US. In the year 2000, credit cards accounted 95 % of online payments and accounted $47 billion of credit cards transactions in the US. This figure rosé to $25 trillion in the year 2004 (Federal Reserve Payment Study, 2004). However, according to Jupiter Media Matrix Research Survey, some consumers would prefer to other payment system, such as e-cash, debit cards and e-chequing.

[64] Lawerence, Stacy (2000), *"Study Peeks into Worldwide Wallets"*, The Industry Standard, April. pp 34-54.

Section II

Securing the Electronic Payment System

The lack of security and trust has been repeatedly reported in market analysis as one of the most important factors hindering the development of e-commerce. As electronic payment system increased the opportunity for the fraud on the web, security is becoming an important component of the electronic payment systems. Section II mainly aims to study the security schemes for securing the electronic payment systems. This section discusses the security provisions of the electronic payment system. The present section deals with both technological and non-technological procedures/measures, which can be used to counter each type of the threats relating to the electronic payment system. At the end, concluding remarks are given.

Over the past ten years there have been hundreds of electronic payment systems-some representing new forms of money, other are re-inventions of old-that have sought commercial acceptance. The list is long and notable for its success and failures (Tumin, 2002)[65]. Whatever, be the payment system, security is the biggest issue of concern and most desirable feature of any payment system. But, this is especially true in the context of electronic payment system, as the chances of fraud (Table: 1) are really very high in electronic payment system in comparison to the traditional payment system. The payment information can be stolen or altered in a number of ways by the cyber criminals[66]. Once this[67] is found out, the information can then be used to purchase other goods online for delivery to a temporary or at the fake address. By the time, the fraud is detected; the criminals would have disappeared from the spot. This fear of losing financial information over the Internet frequently prevents users from making purchase online[68]. Study of KPMG (2002)[69], reported that security of credit card[70] numbers and personal information were by far the most important concerns to their customers. Further, Computer Crime Report (2004) presents a shocking picture of financial fraud.

[65] Tumin, Zachary (2002), *"The Future Technology of Money"*, in OECD *(ed.)*, The future of Money, France: Organization for Economic Co-operation and Development, pp. 73-89.

[66] Various studies (Norton, 2003; Computer Crime Report, India, 2002) indicate that most of the time theses people are from inside the organization or the people who deals with the electronic payment system in any organization.

[67] For example in the case of credit card, the name of card holder, name of company, name of credit card Company, credit card number and expiration date etc.

[68] However, this fear appears to be largely unfounded. Real incidence of losing credit card information are much lower than the users generally thinks. For instance, a study conducted by the ActiveMedia Research, the 58% of consumers reported a fear of online credit card theft, when only a 2 % occurrence was reported.

[69] KPMG (2002), E-Fraud Report accessed on http://www.kpmg.com

[70] The most common cause of credit card fraud is lost or stolen card that is used by someone else; followed by employee theft of customer numbers and stolen identities criminals applying for the credit card using false identities.

Table 3.1: Picture of Financial Fraud

Year	Respondent	Lowest Reported.	Hghest Reported.	Annual Loss	Total Loss
1997	26	$5K*	$2M**	$9,57,384	n/a***
1998	29	$1 K	$2M	$3,88,000	$27,86,000
1999	27	$10 K	$20M	$14,70,592	$3,55,000
2000	34	$500 K	$21M	$16,46,941	$82,47,500
2001	21	$50K	$40M	$44,20,738	$42,83,600
2002	25	$1K	$50M	$46,32,000	$1,83,70,500

* In thousand (000);** million (0000);*** not available

Source: CSI / FBI Computer Crime Report 2002.

Thus electronic payment systems have become the target of rising fraudulent activities[71] by individuals and sophisticated gangs who would like to take advantage of any gap in security. The techniques involved in this criminal process are: spoofing[72], sniffing[73], content alteration[74], and denial of services[75]. Thus, there are many areas where risk related to payment system exists. Therefore, there is a strong need to address these serious issues for making electronic payment system safe and secure.

Securing Electronic Payment System

As electronic payment system increased the opportunity for the fraud on the web, security is becoming an important component of electronic payment system. One challenge electronic commerce retailers face is providing payment mechanisms that consumers perceive as sufficiently secure and convenient for making payment to induce them to complete commercial transaction online. Many alternative ways have been proposed or are now in use for providing secure and convenient payment for the Internet transaction, but none has anywhere near the acceptable that the paper and coin based currency have today. For electronic commerce to grow beyond a small niche market, ordinarily consumers will have to be persuaded to accept some form of digital payment mechanism as being reliable and convenient to use as cash in today. There are number of security schemes (both technological and non technological) to develop fundamental trust among the consumers, retailers, and service providers that is necessary for the electronic payment to function (Westland & Clark, 2001)[76].

---

[71] Laudon and Traver (2003)

[72] Hackers can spoof configure, a system to masquerade as another system, thus gaining unauthorized access to resources or information on system that 'trust' the system being mimickers. A hackers may assume someone else's identity, whether it be a login ID, an IP Address, a server or an e-commerce e-merchant or he/she may perform the act of mimicking a legitimate website including layout, colours and function to obtain credit card information or steal business information.

[73] A sniffer is a type of eavesdropping program that monitors information travelling over the network. When used legitimately, sniffer can also help in identifying potential network trouble spots, but when used for the criminal purpose, they can be very damaging and very difficult to detect.

[74] A method involved in diverting payments would be to intercept a bank account number and change it to another. This is called content alteration. Sniffer who are involved in this, capture the packets, after the content and then send the new packet to its intended recipient.

[75] In the denial of service attack, hackers flood website with useless traffic to inundate and overwhelm the network. DoS attack may cause a network to shut down, making it impossible for users to access the site.

[76] Westland, J. Christopher and Clark, H. Theodore (2001), *Global Electronic Commerce: Theory and Practice*, New Jersey: University Press, p. 465.

The present section deals with the technical procedure, which, can be used to counter each of the threats[77] relating to electronic payment system. In this respect, there is a widespread assumption that common focus is on public key infrastructure (PKIs), digital signature, digital certificate, public key cryptography and firewall and some Internet payment system will lead to secure and trustworthy environment for electronic payment.

Public Key Infrastructure (PKI): PKIs provide a systematic framework to generate, distribute, and maintain the cryptographic key pairs[78] required for achieving properties like authentication, authorization, data confidentiality, data integrity, non-repudiation of communications over Internet, which, are the most basic security requirements for online payment system (European Commission, 2002)[79].

---

[77] Fajor (2004) identified the following threats relating to the electronic payment system:

1. *an individual can break into an electronic system in order to intimate unauthorized transactions on another individual's legitimate account, thereby stealing money.*
2. *that individual can also steal customers personal data, enabling the wrongdoer to set up illegitimate credit card account, bank account and other account-this is called identity theft.*
3. *that person can attack or corrupt the data in the electronic system, either as vandalism or to extort money from the sponsoring financial institution.*
4. *they can also take advantage of the convenience and speed of the electronic system to mask illegitimate or illegal transactions-i.e., money laundering.*

It is also useful to consider not only these specific threats, but also the underlying themes that are of particular concern in recent years. Three such themes are terrorism, identity theft and internal fraud.

[78] There are two types of cryptographic keys: single key cryptography or secret key cryptographic and public key cryptography. Both systems follow a simple set of principles in their design. For example in case of single key cryptography- assume 'A' wants to send a message to 'B' and do not want that anyone except 'B' read this massage. 'A' "encrypt" or "encipher" the message, scrambling the information content so that it is unreadable to anyone except 'B' the intended recipient. In this process 'A' supply a "key" or password to encrypt the message, and 'B' have to use the same key to decipher or "decrypt" it (see figure 3.8). This is the simplest way to secure message. The primary weakness in a single key system is that the key must be transmitted via secure channels so that both parties can know it. If you already have a secure channel for transmitting information, then you do not need encryption. In practice, the key is sent over an unsecured but different channel.

Public key cryptosystem: security can be greatly improved by the use of public key cryptosystems. In such systems the sender and receiver of message have two related, complementary keys, a publicly revealed key and a private key (which is kept secret). Each key unlocks the code that the other key makes (see figure 3.9). To transmit secure message, the sender encrypts his/her message with the public key of the intended recipient. The recipient decrypts that message with his/her own secret key. Indeed, the only key that will decrypt the message is the private key, which was generated with the public key used to originally encrypt that massage.

[79] European Commission (2002), *Securing Payment over Internet,* Institute for Prospective Technological Studies, Report EUR 20263 EN.

Figure 3.8: Private Key/Single Key Cryptography

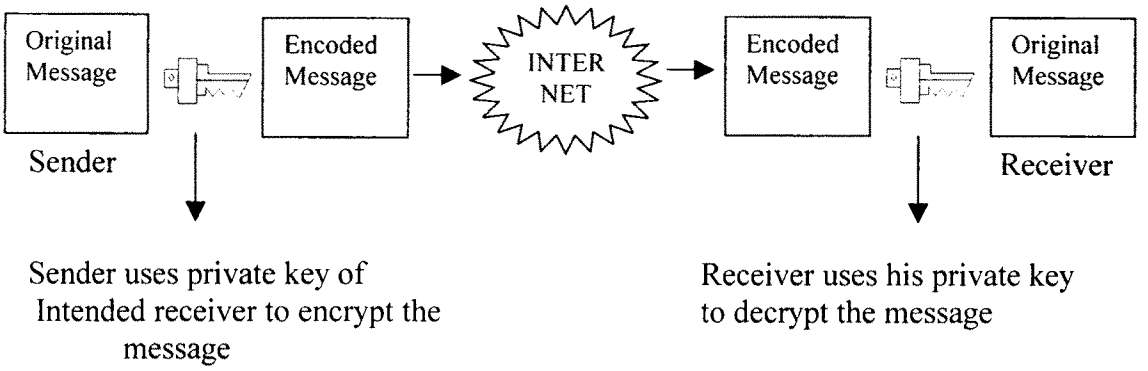
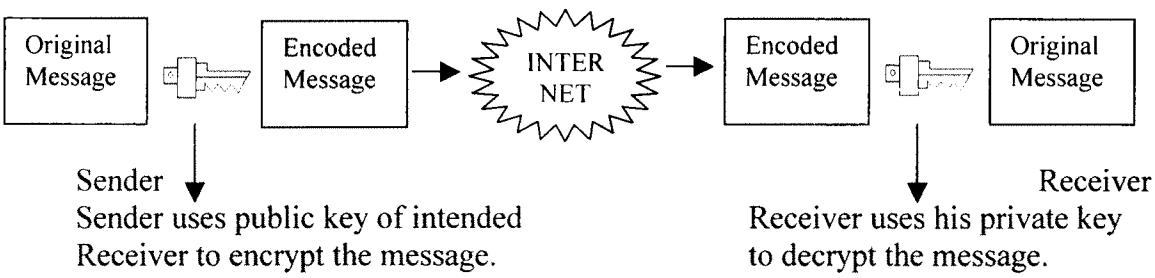


Figure 3.9: Public Key Cryptography



These frameworks uses as data structure, called digital certificate, to populate user's cryptography key and other credentials (Patil and Shyamasundaram, 2005)[80]. Thus, PKI is much broader term. It encompasses secure hardware and software, security mechanisms, operational rules, organizational practices, contractual terms and liabilities, and further elements. It enables additional necessary functions for e-commerce such as time stamping, documents notarization, secure e-mail and digital proof of receipts. On Internet, PKI is used in two different ways as a secure payment system:

- ***Secure Socket Layer Protocol (SSL)***: secure socket layer protocol developed by Netscape Communications allows, a secure connection or information 'tunnel' between the web browser and a web server, based on a combination of public key cryptography and faster symmetric cryptography for encryption/decryption[81]. This protocol provides confidentiality and integrity of the data exchanged between the consumer browser and the merchant server. SSL is simple, cheap and quick to implement, and, in combination with credit card data introduced through PC keyboard, is the most used "payment instrument" on the Internet[82]. However, SSL only protects the link between the browser and server, but does not protect that data once it is collected by the merchant server, where most

[80] Patil, Vishwas and Shyamasundaram, R.K. (2005), *"Trust Management for E-Transactions"* Sadhana Vol. 30, N0. 1&2, pp. 141-158.

[81] This is to overcome the high computational resources required by the asymmetric cryptography, which makes it impractical for encrypting/decrypting large amount of data.

[82] Communication by Russ Jones from CommerceNet estimates that close to 99% of web sites accept credit card data entry used SSL.

attacks take place. It is also true that a number of (SSL) validation processes are done without the consumer's awareness[83] or intervention.

- ***Secure Electronic Transfer Payment Protocol (SET)*:** the SET specification is an open technical standard for the commerce industry, developed by Visa and MasterCard to allow secure credit card transactions over the Internet. The use of digital certificate, signatures and PKC creates a trust chain throughout the transaction, provides consumer and merchant authentication, data confidentiality and integrity and non-repudiation capability[84]. A particular feature of the SET protocol is that through the use of specific cardholder, acquirer and merchant certificates, payment data is protected from merchant access. Its subsequent storage at the merchant server is thus avoided, along with the risk of it being stolen.

Public Key Cryptography (PKC): a more powerful form of cryptography involves the use of public keys (Kalakota and Whinston, 1996)[85]. A key advantage of PKC[86] is that it permits individuals to use two different but related keys to authenticate each other and maintain the confidentiality and integrity of their communications. It also allows them to digitally sign[87] a document or a transaction. One key, the private key is kept secret by the owner, while the other, the public key, can be widely distributed. The two keys are mathematically related, but an important feature is that it is computationally unfeasible to derive one key from the knowledge of the other; PKC provides an easy mechanism for the data encryption and integrity (e.g., SSL). The authentication of these parties, however, requires a trusted third party or a trust chain (e.g., PGP). A third party is also necessary to legally bind a digital signature to the signing party and to enforce non-repudiation.

Public key cryptography is very useful because network security based on the public key techniques tend to be more easily configurable. Public key cryptography might be used in the beginning of communication for authentication and to establish a temporarily shared secret key, then the secret key[88] is used to encrypt the remainder of the conversation using secret key techniques (Kanfman *et al,* 2003)[89]

---

[83] For example only a small number of consumers are aware of the significance of the locker at the bottom of the screen, take active action to configure, verify, accept or reject merchant web site certificates, understand the purpose of the public/private key stored on his PC etc.

[84] However, enforcement of non- repudiation depends on the contracts established between banks and consumers and markets under the prevailing national; laws.

[85] Kalakota and Whinston (1996)

[86] PKC is sometimes also referred to as asymmetric cryptography.

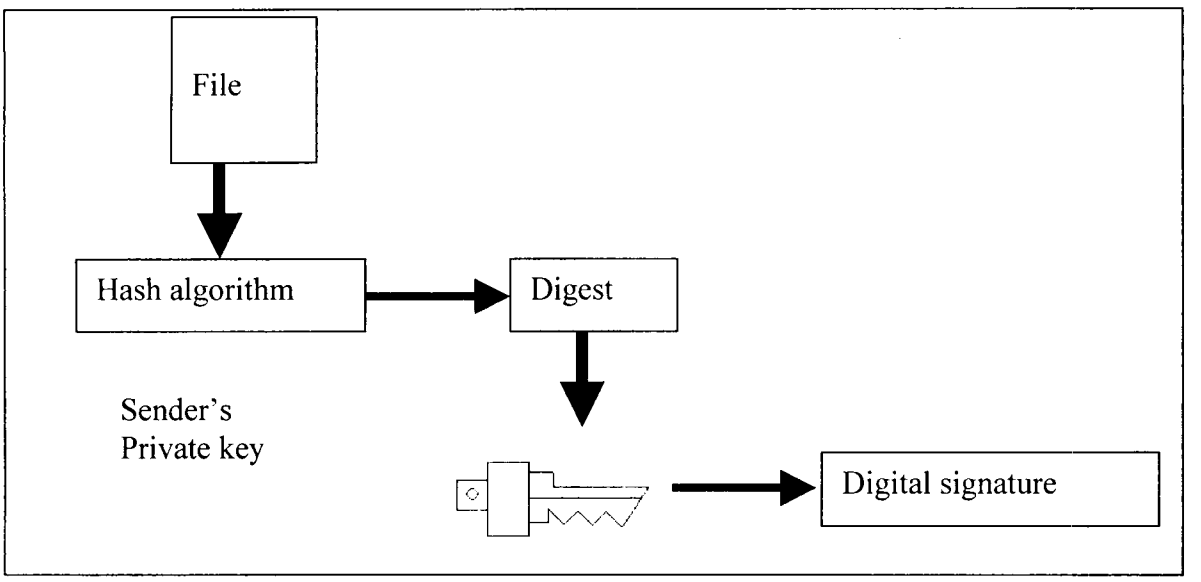
[87] It can also be used for sender authentication, known as digital signature.

[88] Some people use the term secret key for the private in the PKC or use the term private key for the secret key in secret key technology. But there is difference between these two. The term secret key is used as the single secret number used in secret key cryptography. The term private key should refer to the key in public key that must not be made public.

[89] Kanfman, Charlie; Perlamn, Radia and Mike, Speciner (2003), *Network Security: Private Communication in a Public World,* New Delhi: Pearson Education.

Digital Signature: a digital signature in the electronic world (e.g., in an exchange of payment information) provides same kind of characteristics[90] that are expected from a handwritten signature in the paper-based world. It is applicable to providing authentication of the signer, integrity of information being signed and non-repudiation of the transaction. Digital signatures are being used for the protection electronic payment, exchange of information via web browser, filing tax records and other legal documents, online shopping and transactions (Humphreys *et al,* 2004)[91]. The term digital signature refers to a signature that can be calculated by making the use of hashing techniques and public key encryption to ensure the integrity of a document and authenticate its source[92]. In a very simple term digital signature is created by using special software which:

Figure 3.10: Components of Digital Signature



-Converts the electronic message, file or data into a mathematical summary (hash or digest) using a special mathematical algorithm (hash algorithm).
-This digest is then encrypted using the originator/sender's own private key.
-This then creates an encrypted value, which is the digital signature. Each digital signature is different each time it is used on a different and new message (Tassabehji, 2003)[93].

[90] Digital signature can be used to authenticate the identity of the originator of the message in a similar way that handwritten signature authenticate the signer. By sending a message or receiving a message that is digitally signed, the sender or the receiver cannot later deny having sent it because the digital signature is unique to each individual user.

[91] Humphreys, Ted; Marijke De Snete and Chris, Mitchell (2004), " *Securing E-Business*", ISO Focus, January.

[92] This is used in the line with the (ISO/IEC 7498-2) definition for digital signature, "data appended to, or a cryptography transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery, e.g. the recipient.

[93] Tassabehji, Rana (2003), *Applying E-Commerce in Business*, London: Sage Publications.

Digital signature has a multitude of applications, including electronic fund transfer (EFT), Electronic data interchange (EDI), contracts, authentication and certification. To be widely accepted for critical business task, digital signatures must have characteristics similar to written signatures. They must be easy to produce, easy to recognize and difficult to forge. Digital signatures also must serve as a mechanism for electronic signatures that binds the maker to the record in a tamper-evident package (Rafeo, 2001)[94]. They make it possible to demonstrate to the third party that the maker signed the record and that the content has not been changed.

Digital Certificate: Rather than being protected from exposure, public key's are widely disseminated. Therefore, it is important to protect public keys from being tampered with, to make sure that a public key really belongs to whom it appears to belong to[95]. A better and trusted way of distributing public keys is to use a certificate authority[96]. A certificate authority maintains the responsibility for checking user's identity, issuing digital certificate, and verifying the validity of digital certificate.

A digital certificate is an electronic identification card that establishes a user's authenticity in the electronic world. The digital certificate (conceptually similar to credit card) contains information, such as name, e-mail address, a serial number, expiration dates, a copy of certificate holder's public key and the digital signature of the certificate- issuing authority so that a recipient can verify that the certificate is real.

In Internet based transactions, digital identification takes place invisibly through the software built into the browser, and via icon clicks. The US based company Verisign uses a relatively standard approach that offers several classes[97] of security (Westland and Clark, 2001).

Firewalls: the most commonly accepted network protection is a barrier-a firewall[98] [99]-between the corporate network and the outside (untrusted) world (Kalakota and Whinston, 2004)[100]. A firewall protects networked computers from intentional hostile intrusion that could compromise confidentiality or result in data corruption or denial

---

[94] Rafeo, A. (2001), *"Signing on the Electronic Line"*, E-Commerce, Vol.1, No. 4, pp 22-24.

[95] Westland, J. Christopher and Clark, H. Theodore (2001), *Global Electronic Commerce: Theory and Practice*, New Jersey: University Press.

[96] With digital certificate, a certifying authority (rather than the individual) generates the public and private keys at the request of an individual contracting the services of certifying authority. Both keys are returned on the certifying authority's database, under the certifying authority's control.

[97] A Class1 certificate verifies only e-mail address, by e-mailing a personal information numbers that the user must enter into the registration. A Class 2 certificate provides to websites on demand, the holder's real name, which Verisign has confirmed by checking name, address, US security number, and other information against a credit bureau database. A Class 3 certificate is available to the companies; corporate employees go to a Verisign office and present photo identification.

[98] The concept of firewall comes from the fact that by segmenting a network into different physical sub-networks, they limited the damage that could spread from one subnet to another just like firedoors or firewalls.

[99] Bruce Schnier explained the origin of the term firewall (Bruce, Schnier (2000), *Secret and Lies- Digital Security in a Networked World,* John Wiley & Sons.

[100] Kalakota, Ravi and Whinston, B. Andrew (2004), *Frontiers of Electronic Commerce,* Singapore: Pearsons Education.

of service. It may be hardware, software, or a combination of both running on a secure host computer (Ravi, 2001)[101]. A firewall works closely with a router[102] examining each message or packet, and blocking those that do not meet the criteria specified in the firewall configuration.

There are two access denial methodologies used by firewalls. A firewall may allow or deny all traffic unless it meets certain criteria. The types of criteria used to determine whether traffic should be allowed through varies from one type of firewall to another. Firewall may be concerned with the type of traffic, or with source of destination addresses and ports. They may also use complex rule base that analyze the application data to determine if the traffic should be allowed through. How a firewall determines what traffic to let through depends on which network layer it operates at[103].

Firewall comes in several types and offer various level of security. Generally, there are four kinds of firewalls: (1) the network level firewall, which is one of the most common and functions like a packet filter system (2) proxy of application level firewall, this kind of firewall adds more layer of security. Schneier compares it to placing a guard inside the castle walls and another outside the walls (3) a demilitarized zone (DMZ), coined from the setting up of a buffer zone as a result of the conflict between North and South Korea in the 1960s, describing the use of two firewalls to protect an area of network which consists of dispensable public service (Tassabehji, 2003)[104].

Non-technological Measures for Securing Electronic Payment

Despite existing security standards and security technologies, such as secure hardware gap between users' demand for security and the security offered by a payment system can still remain[105]. These security gaps imply risks for the users. Indeed, there is high risk in electronic payment system and alone above-mentioned technologies cannot remove all risks. So the consumers (users) should be alerted to these risks. There are some general guidelines for both the users and for the companies. A user should consider the following suggestions for safe and secure online payment experience.

- Read the privacy statement[106] of vendors, especially in the case of where consumers are not familiar with the vendor; verify the validity of information, as well as reputation of the company (Gupta, 2003)[107].
- Consumer should give credit card details only over a secure connection. Consumer can check this in three ways. First, the address will be given in https rather than http. Second, a padlock symbol will appear at the bottom of the browser window. Third, messages will pop-up when consumer switches between a secure and non- secure site, although this can be disabled.

---

[101] Ravi, R. (2001), *"The World of Firewalls"*, E-Commerce, Vol.1, No. 3., pp 40-43.

[102] A router is a device or software that determines the next network point to which a packet of data should be forwarded route to its final destination.

[103] Ravi, R. (2001), *"The World of Firewalls"*, E-Commerce, Vol.1, No. 3., pp 40-43.

[104] Tassabehji, Rana (2003), Applying *E-Commerce in E- Business*, London: Sage Publication.

[105] Report of OECD (2002) on *Guidelines for Consumer Protection in the Age of Electronic Commerce*

[106] A privacy statement is the legal binding document that describes the personal information and dissemination practices of a web site.

[107] Gupta, Krishma (2003), *"Caveat Emptor: Consumer Beware"*, E-Commerce, pp.36-37.

- Never send credit card details by e-mail. Pay attention to credit card billing cycles, and follow up the creditors if bill do not arrive on time (Sumanjeet)[108]. This could be a sign that someone has changed the address or other information from the consumer file to hide illegal changes from consumer.
- Make a print out of all the web pages or e-mail directly related to the purchase, so that the consumer will have complete records on the event of any problem.
- When making payment online, check the lock or icons on the screen to make sure that the site is secure. A broken icon indicates that the site is not secure.

Added to theses guidelines, there are some general guidelines suggested by various banks [109]to their customers regarding the use of plastic money. These are:

- Sign on the signature panel of the debit card immediately upon the receipt. And protect the magnetic strip from the exposure to direct sunlight, magnets and scratches.
- Never keep a copy of PIN (Personal Identification Number) in wallet and never write PIN number on the card.
- Keep a photocopy of front and back of card.
- In case the card is stolen/misplaced[110] call bank help line to inform about the same.
- Keep the charge slips safe, to tally them against the billing statement.
- Never have PIN or passwords, which are easily identifiable by the others like your name, date of birth and your car number etc.

Guidelines for Companies: Security is not a consumer problem, in real sense it is a business problem. Therefore it is the responsibility of every company to provide an environment where their consumers can feel safe and secure regarding the payment issue. There are some guidelines for companies to make their online customer safe regarding the payments.

- There are large numbers of payment systems at hand or at least on trail. Identifying the common risks involved in the various online payment systems is the first step towards securing payment. In order to identify common risks, payment systems must be classified. There are several proposals of how to do this, which can be summed up in a generic concept. Payment system can be distinguished, e.g., upon the time of value transfer, the binding to account processing, the kind of payment information communication and initiation of value transfer.
- Each business needs to clearly spell out its security policy, procedures and practices for implementing the desired level of security, and enabling the

---

[108] Sumanjeet (2004), *"Consumer Protection in the Age of Electronic Commerce"*, The Business Review, Vol. 11, No. 1, pp 111-116.

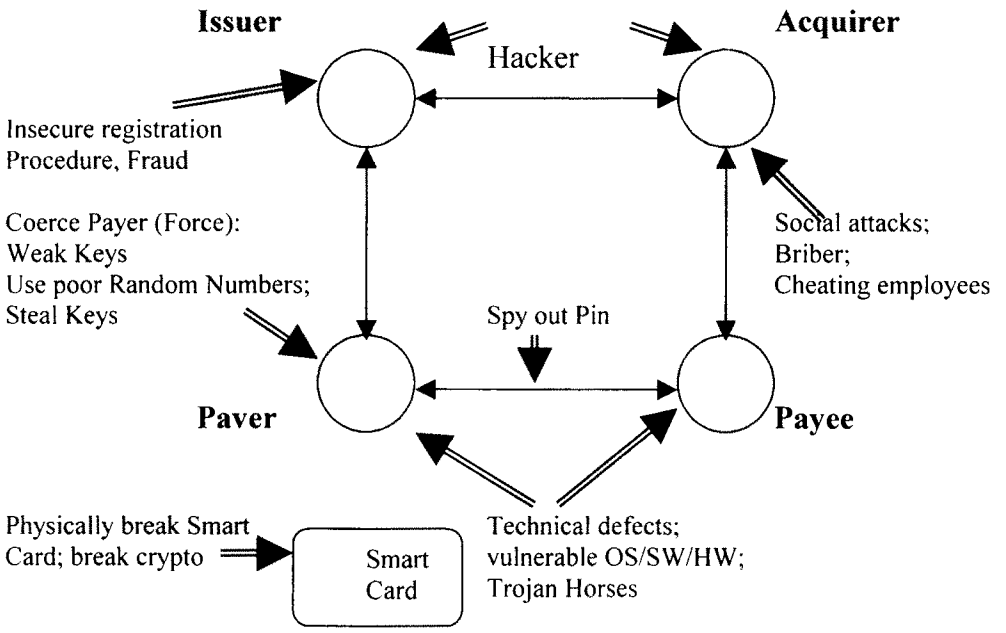
[109] Various Indian Banks such as UTI BANK, HDFC, ICICI and SBI suggest these guidelines. These guidelines are compiled by the researcher on the basis of the contents of the advertisements of the said banks.

[110] However, some banks are providing zero liability cards. It means, if your card is stolen or misplaced, just do not worry. With the zero liability cards you are fully protected against any misuse or unauthorized purchase of your card.

framework of defense mechanism and service configurations. A comprehensive security for e-commerce payment covers security at the host level, the site level and on-the-wire transaction level. Site security includes detection and deterrence against sniffing and spoofing attempts and protection of important services such as web servers, DNS servers, and other infrastructure service (Bhaskar, 2003)[111].

- Generally, the security of complex information systems, such as electronic payment system, can never be absolute. Not all leaks can be known and put right by technical means at the outset. The relationships of parties involved in each transaction are far too complex[112], and points of attack in an open communication system similar to the Internet are numerous (See Figure3.11).

Figure 3.11: Information Flows and Exemplary Potential Points of Attack in a Digital Payment System



Source: Reichenabch *et al,* (2000)[113]

However, security not as some static value, but rather by analyzing the fundamental information flows from a dynamic point of view, is the first step towards handling risks of each participant in the system.

- Security must be economically feasible. Thus, even the theoretically maximal conceivable "technical" security (which we call the largest achievable security level) need not necessarily be implemented. Increasing usage of technical means is combined with the decreasing rates of growth of security scale, and thus with

[111] Bhaskar, Bharat (3003), *Electronic Commerce: Framework, Technologies and Applications, New Delhi: Tata McGraw Hill.*

[112] Note that all parties involved must be considered, i.e., payer, paye, issuer, acquirer, credit card companies, trusted third parties, and so on.

[113] Reichenbach, M; Grzebiela, T. and T. Koltzsch, I. Pippow (2000), "Individual Risk Management For Digital Payment", accessed on http://econwpa.wustl.edu/eprints/comp/papers/0204/0204001.abs

disproportionate increase in the costs[114](Petzel, 1998[115] and Damm & Menge 1999[116]).

- Risk can also be reduced economically by involving intermediaries. On the one hand the intermediaries can help to recognize risks and thus yield increased transparency. These intermediaries can also work as supervisory and also can analyze, judge, and certify the security of the digital payment system[117] (Hamamtoglou, 2005)[118].
- The risk can also be transferred by the company to the third party by insurance, a traditional economic tool. The insurer will bear a specified risk during a particular period of time (Farney, 1999)[119].
- Last but not the least; risk can be distributed among all the parities (Damker *et al.*, 1999)[120] involved in the electronic payment process. Those who explicitly bear risks like insurer or individual whose adoption level cannot be met to build risk reserves.

Concluding Remarks:

The lack of security and trust has been repeatedly reported in market analysis as one of the most important factors hindering the development of e-commerce. In order to maintain and acceptable level of security and trust when trading on open networks, it is not only necessary to replace the traditional face-to-face mechanism with digital ones but also to create new tools (legal, digital and procedural) to manage the specific risks of an open network environment where e-commerce transactions takes place. All over the world a number of technologies have been developed to handle with the risk of e-payment in e-commerce. Some of the most important and widely used are: digital signature, digital certificate, Public Key Infrastructure, Public Key Cryptography and Firewall. But none of them have anywhere near the acceptance[121] that paper and coin-

---

[114] In this context, security is the result of the use of the security technology. Increasing use of security technology is related with the decreasing marginal revenues of "security". This implies that the cost of each additional unit of security will increase by a factor greater than 1,i.e. that the cost for an additional unit of security technology will stay constant

[115] Petzel, E. (1998), *"Integration von Vericherungen in Sicherhetiskonzepten"*, Lecture on the Congress IT- Sicherhetistmanagement 98 in Munchen adopted from Reichenback et al (2000), *Individual Risk Management for Digital Payment System*, Institute of Informatika and Gesellschaft.

[116] Damm, F. and Menge, W. (1999), *"Cost Comparison of Traditional and Alternative Telecommunication Approach"*, in G. Muller and K. Ranneberg (ed), Multilateral Security in Communications Technology, Infrastructure Economy.

[117] In this case the intermediaries can attest fulfillment of very special criteria for one payment system.

[118] Hamamtoglou, A. Weber (2005), *"The Fair Internet Trader"*, in G. Lacoste; B. Pitzmann; M. Steiner and M. Wainder (ed.), SEMPER Final Report, LNCS, Springer, Berlin.

[119] Farney, D. (1995) in Reichenback et al. (2004), *"Individual Risk Management for Digital Payment System"*, Institute of Informatik and Geselleschaft. accessed on http://econwpa.wustl.edu/eprints/comp/papers/0204/0204001.abs

[120] Damker, H.; Pordesch, U. and Reichenback (1999), *"Personal Reachability and Security Management"*, in G. Mullar and K. Rannenberg (ed), Multilateral Security in Communications Technology, Infrastructure Economy.

[121] However, firewall have emerged as an important mechanism for fortifying e-commerce payment security, by controlling access, monitoring, and filtering the incoming and outgoing message traffic, right

based currency have today. Therefore, added to the technological measures for securing electronic payment, some individual and organizational strategies are needed to make the electronic payment environment more safe and secure.

Some Concluding Observations:

- Security of electronic payment in the e-commerce is the biggest issue of concern not only for the developed world where most of the payment are made though Internet; but also for the developing countries like India where very few people are using electronic payment tools like credit cards etc. In the developed world problem of security exists mainly due to high technological advancement whereas in the developing country it is due to the lack of secure technologies and poor awareness among the user and the companies.
- Referring to a number of reports based on empirical data and examination the kinds of network security breaches, it is revealed that Internet infrastructure has many fundamental security design problems that cannot be addressed very quickly.
- As the chances of risks are high and many in electronic payment system; it is quite impossible to eradicate security breaches mainly because of majority of them are as a result of human malice, error or lack of awareness. But this can be minimized by introducing different layers of security in an organization to ensure that, once all the measures are in place, if one layer is breached then the next layer will stand up and so on, until either the impact of the breach is at best detected and disarmed or at worst cause minimum damage.
- Survey reports and personal experience repeatedly shows that many of the security breaches that occur are as a result of people and most of the time they are from the inside of company. Therefore, a general observation regarding the behavior of employees should be considered as important tool of security. However for the best result consumers (users), businesses, software developers and government have to work together to make this new form of payment a reality.
- An appropriate legal framework is very important for the development of this new form of payment. Most of the counties of the world still do not have any law regarding the protection of consumers in the age of e-commerce. Fortunately we (India) do have, but our Information Technology Act, 2000 is silent about the issue of electronic payment system. Therefore there is strong need to introduce new laws regarding electronic payment and amendment is required in the existing laws to create the trust among the users of new payment tools, which is the fundamental condition for security. As there is no boundary in electronic transactions (payments), action at international level is also needed to make the electronic payment a reality all over the world.

---

down to the packet level. The prevention of sniffing, spoofing, and access monitoring and control through firewall can secure a site from unwanted traffic and intrusion attempts.