

Ways of Transacting Online

Mukta Sharma*, Dr. R.B. Garg**

* Research Scholar, TMU

** HOD CS/MCA, Tecnia, IP University, Ex-Prof., Delhi University

Abstract- There is no doubt the Internet is a wondrous creation. The entire world is rapidly becoming obsessed with it. With the advancement of technology, there was a long felt need to give recognition to the electronic means as an alternative to paper based banking. The internet has made banking and other business transactions a lot easier because money is easily transferred from bank to bank, employer to employee, employee to bank, shopper to department store, and almost any scenario in which money has to be transacted, all because of the internet and other electronic technologies.

The worldwide proliferation of the Internet has led to the recent birth of electronic payment system: a payment service solution-software that enables monetary value to be transferred digitally. Parties conducting electronic businesses and transactions have usually never seen each other face-to-face, nor exchanged currency or hard copies of documents hand-to-hand. The society prefers transactions that involve physical contact of people, cash and cheques to that, which is done via a telecommunication network such as the Internet. However, security, trust and convenience are among the major contending factors affecting the adoption of e-payment systems. In this paper, we considered some critical examinations on the existing payment system.

Purpose: The objective of the paper is to understand the various mediums of paying online and variant issues affecting the same, along with few standards of security like-SET, SSL, HTTPS etc.

Design/methodology/approach: To understand the existing medium of paying online and accessing the benefits and limitations for the same.

Findings: The banking sector occupies a pivotal position in the global economy. E-banking is one of the most challenging tasks as it is changing the banking industry and is having the major effects on banking relationships. We are moving from brick & mortar model to click & mortar model. E-banking involves use of Internet for delivery of banking products & services. There are various medium involved to make a secure payment.

Research limitations/implications: Research design is exploratory in nature hence; the results of the study are not very conclusive.

Index Terms- E-Banking, E-Payment System (EPS), Automated Clearing House (ACH), point of sale (POS)

Paper Type - Conceptual Paper

I. INTRODUCTION

Buyers and sellers increasingly want to use the Internet to conduct their business electronically. Consumers will want to use the Internet as a means for multiple phases of the purchase process: searching for suppliers, price negotiation, ordering, and payment for goods. Technology developments and innovations are having a significant impact on the banking industry. Banks face the challenge of adapting, innovating and responding to the opportunities provided by the technological advancements. The growth of e-banking has benefited enormously to banks and their customers. It has allowed banks to expand outreach, reduce transaction costs, improve efficiency, and provide virtual banking services. On the other hand, customers have benefited from efficient banking services at relatively lower costs and having the option to choose from alternate delivery channels. The e-banking has also facilitated swift movement of funds domestically and across borders.

We have known money as a medium of exchange to simplify transactions & to decide the worth of goods. E-money is an electronic medium for making payments and is the trend today. People are moving from paper-based money to plastic money. This changing financial landscape has posed new challenges for banks and policymakers/supervisors. Banks now have increased reliance on technology to compete in an increasingly competitive business environment and thus need to effectively manage the IT security and other related risks. Banks have to focus on the various e-payment System. E-payment scheme allows two users to securely exchange e-cash and digital product over an open network. Today, electronic payment system is flourishing due to the openness, speed, anonymity, digitization, and global accessibility characteristics of the Internet, which has facilitated real-time payment transactions and other business activities.

II. TRADITIONAL BANKING

Traditional payment methods include cash, cheque, credit and debit cards. These methods have several shortcomings.

- Cheque and cash cannot be exchanged in real time
- Credit and debit card info exchanged over the phone or by email entails security risks
- Some individuals do not have access to credit cards or checking accounts because of credit history.
- The overhead of all but cash do not support low value transactions (micropayments)

There are many problems with the traditional payment systems enumerated below:

(a) Inconvenience:

Traditional payment systems require the consumers to either send paper cheques by snail-mail/ via some one to handover the cheques 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/ modified by anyone.

(c) Lack of Coverage:

When we talk in terms of current businesses, they span many countries or states. These business houses need faster transactions everywhere. This is not possible without the bank having branch near all of the companies' offices.

(d) Lack of Eligibility:

Not all potential buyers may have a bank account.

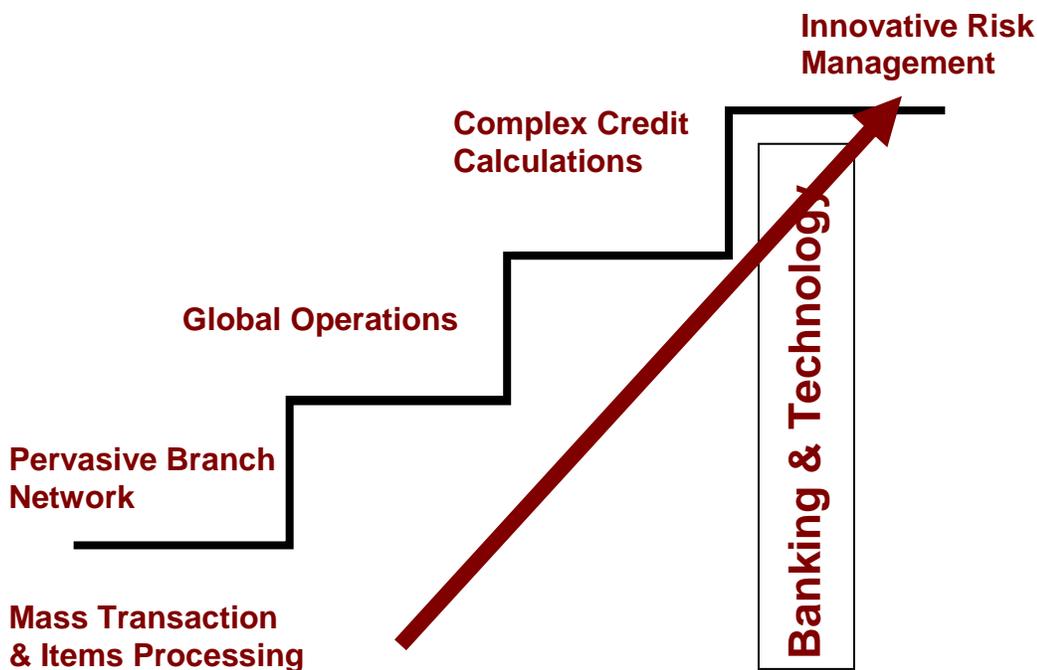
(e) Lack of support for micro-transactions:

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.

III. E-BANKING

“Electronic Banking” or “e-banking” is an umbrella term for the process by which a customer may perform banking transactions electronically without visiting a branch and includes the systems that enable customers of banks, individuals or businesses, to access accounts, transact business, or obtain information on financial products and services through a public or private network, including the Internet.

E-banking is defined as the automated delivery of new and traditional banking products and services directly to customers through electronic, interactive communication channels. E-banking includes the systems that enable financial institution customers, individuals or businesses, to access accounts, transact business, or obtain information on financial products and services through a public or private network, including the Internet. Customers access e-banking services using an intelligent electronic device, such as a personal computer (PC), personal digital assistant (PDA), automated teller machine (ATM), kiosk, or Touch Tone telephone.



Advantages of Using E-banking

(i) Convenient

E-banking is convenient because we can use e-banking for tracking money in bank without going to bank. It saves time and is lot more easier.

(ii) Protection of Environment

E-banking, protects environment and is much cheaper.

Suppose, customer have to withdraw money from a bank and deposit it to another bank. He/ She has to commute via some vehicle. By using vehicle, you are increasing the pollution in the

environment. You can also use e-bill facility of your Internet bill.

Earlier customer use to maintain passbook to see every transactions, which customer have made in recent past. This leads to cutting of trees (as paper is made from tress). Now you do not have to get it printed or manually updated. You can see it online by log in to your account or you can get a message on your cell communicating you about the immediate transaction & available balance. It is a paperless environment. we can call this as green environment.

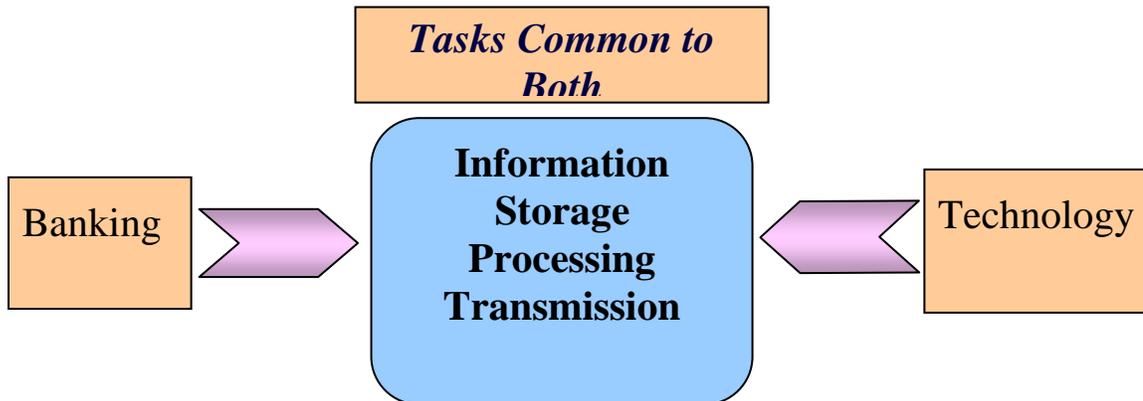
Disadvantages of Using E-banking

Hacking, Phishing, spyware program, computer virus and breaking online password are the weakness of e-banking or online banking. Online big hackers are using computer virus and after spreading it, they compromise your computer. After this, they know all detail of your computer and banking password and

illegally transfer all your money. Even you can stop this crime by writing strong password but you cannot remove it totally.

IV. TECHNOLOGY AND BANKING

The Quintessence Nature of Banking harmonizes closely with Technology –



Many Benefits of Technology

- Increased operational efficiency, profitability & productivity
- Superior customer service
- Multi-channel, real-time transaction processing
- Better cross-selling ability
- Improved management and accountability
- Efficient risk management
- Minimal transaction costs
- Improved financial analyses capabilities

Not only employees, there are problems for customers too when a new technology arrives.

Issues with Customers

- Comfort levels
- Security and trust issues
- Convenience factor
- Getting rid of myths
- Migration from existing to new systems
- Changing the habits
- Electronic Payments system

An Electronic Payments system means ensuring payment security, transaction privacy, system integrity, customer **authentication**, and the purchaser's promise to pay [3]. Electronic payment system is a mechanism of transferring money over the Internet and technology used in this transfer is called as EFT. The main objectives of EPS are to increase efficiency, improve security, and enhance customer convenience an ease of use. Although these systems are in their adolescence age, some significant development has been made. There are several methods of electronic payments system such as Electronic cash, software wallets, smart cards, and credit/debit cards.

Advantages of E-Payment

- **Increase payment efficiency**
 - Reduce transaction costs
 - Enable trade in goods and services of very low value
- **Increase convenience of making payments**
 - Payment can be made swiftly and remotely using various devices
- **Can be used for**
 - e-commerce / e-Trade
 - For other purposes like paying bills, taxes, etc

Categories of EFT

- **Banking and financial payments**
 - Large-scale or wholesale payment
 - Small scale or retail payment
 - Home banking
- **Retailing payments**
 - Credit cards
 - Debit cards
- **On-line electronic commerce payments**
 - Token-based payment system
 - Electronic cash
 - Electronic checks
 - Smart cards or debit cards
 - Credit card-based payment systems
 - Encrypted credit cards
 - Third-party authorization numbers

An ecommerce environment, a bank, or any financial institution with a payment system needs a complex design. A payment system means ensuring payment security, transaction privacy, system integrity, customer authentication & the purchaser's promise to pay. There are distinct set of properties, which we need to consider during money transfer.

ACID Test

Atomicity states that modifications must follow an “all or nothing” rule. Each transaction is said to be “atomic.” If one part of the transaction fails, the entire transaction fails. A transaction must occur completely or not at all.

Consistency states that all parties involved in transaction must agree to exchange. In a customer-retailer relationship involving a purchase, the customer must agree to purchase the goods for a specific price & merchant must agree to sell it at that price; otherwise, there is no basis for exchange.

Isolation means each transaction must be independent of any other transaction and be treated as a stand-alone episode.

Durability ensures the last committed state or reverses the facts of the exchange. This means reversing charges in the event that customers change their mind.

ICES TEST

Interoperability- Must be interoperable or exchangeable for other digital cash, paper cash, goods or services.

Conservation- Must be storable and retrievable

Economy- Must have a monetary value. Per transaction, cost must be small enough that is insignificant.

Scalability- Ability of the system to handle multiple users at the same time.

In addition to ACID & ICES test, other properties important for an EPS are-

Security- The infrastructure supporting electronic commerce must be usable and resistant to attack.

Reliable- The infrastructure must be highly available and should not present a single point of failure.

Flexible- Different models (credit, cash, cheque etc) for different situations, Need for a common framework.

Computational efficiency- Micropayments, frequent payments for small amounts must be supported. Merchants & payment servers must be able to handle the load.

Unobtrusiveness- Users must be able to monitor their spending and they also should be controlling when, to whom and how much is paid. They should not be interrupted to provide payment information.

V. TYPES OF EPS

The electronic payment systems are proliferating in air ticketing, insurance, banking, retail, health care, online markets and even government. Organizations are motivated by the need to deliver various kinds of products and services. More cost effectively and to provide a higher quality of service to customers.

Internet based Payment System Models- As compensation for information, goods and services provided through the internet are Access to copyrighted materials, Database search, Consumption of system resources etc. Online buyers may use one of the following EPSs to pay for products/services purchased online [12]:

- **Electronic funds transfer (EFT):** EFT involves electronic transfer of money by financial institutions. It is one of the oldest electronic payment systems. EFT is the groundwork of the cash-less and check-less culture

where and paper bills, cheques, envelopes, stamps are eliminated. EFT is used for transferring money from one bank account directly to another without any paper money changing hands. The most popular application of EFT is that instead of getting a paycheck and putting it into a bank account, the money is deposited to an account electronically. EFT is considered to be a safe, reliable, and convenient way to conduct business. The advantages of EFT contain the following:

- Simplified accounting
- Improved efficiency
- Reduced administrative costs
- Improved security
-
- **Payment cards:** They contain stored financial value that can be transferred from the customer's computer to the businessman's computer.
- **Credit cards:** They are the most popular method used in EPSs and are used by charging against the customer credit.
- **Smart cards:** They include stored financial value and other important personal and financial information used for online payments.
- **Electronic money (e-money/e-cash):** This is standard money converted into an electronic format to pay for online purchases.
- **Online payment:** This can be used for monthly payment for Internet, phone bills, etc.
- **Electronic wallets (e-wallets):** They are similar to smart cards as they include stored financial value for online payments.
- **Micro-payment systems:** They are similar to e-wallets in that they include stored financial value for online payments; on the other hand, they are used for small payments, such as kurus in Turkey.
- **Electronic gifts:** They are one way of sending electronic currency or gift certificates from one individual to another. The receiver can spend these gifts in their favorite online stores provided they accept this type of currency.

Above-mentioned EPS have some overlap among them. Since the e-banking is a growing and maturing segment. We have four main models to illustrate internet based systems are electronic currency, credit cards, debit cards, and smart cards.

Cyber Cash- This concept was given by Bill Melton & Dan Lynch in year 1994. They formed Cyber cash Inc. (www.cybercash.com). This was acquired by VeriSign. VeriSign was later acquired by PayPal and recently PayPal has been acquired by eBay. Cyber cash model makes safe passage over the Internet for credit card transaction data. They take the data sent to them from the merchant, and pass it to the merchant's acquiring bank for processing. Except for dealing with merchant through Cyber Cash's server, the acquiring bank processes the credit card transaction as they would process transactions received through a point of sale (POS) terminal in a retail store. Cyber cash servers act as a gateway between the merchant on the

internet and the bank's secure financial networks. The company offers a range of e-commerce solutions, from credit card based payment to secure micropayment system.

- Cyber cash offers services for businesses
- Cyber cash also offers a wallet for users
- Everything is authenticated
- Supports major credit cards as well as debit and purchase cards
- Flexibility to process offline orders
- Automatically logs every transaction including sales, credits, and voids
- Fast transaction processing speed for large volumes
- All transactions are encrypted and digitally signed
- Customers are notified in "real time" of rejection/approval of transactions

Net Bill- This method uses internet for purchasing goods and services and is a secure and economical payment method used mainly for Micropayments. The Net Bill server maintains accounts for both consumers and merchants, which allows customer to pay merchants for goods to be delivered. The goods are delivered in encrypted form to the consumer's machine. The Money Tool software verifies receipt and the goods are automatically displayed for the consumer. The Net Bill protocols enable communication between Money Tool, the merchant server and the Net Bill Server.

Credit Card- A credit card is a small plastic card issued to users dealing in e-commerce. Most credit cards are the same shape and size, as specified by the ISO 7810 standard. A credit card is different to a debit card in that it does not remove money from the user's account after every transaction. In the case of credit cards, the issuer lends money to the consumer (or the user) to be paid to the merchant.

Customers who purchase any goods send their credit card details to the service provider involved and the credit card organization will handle this payment. Online credit card payment has following categories:

- Payment using plain credit card details
- Payments using encrypted credit card details
- Payment using third-party verification

Entities involved in Credit card Transaction

- Consumer (Buyer or Card holder)
- Merchant (Seller)
- Card Issuer (Consumers' Bank)
- Acquirer or Principal (Merchant's Bank)
- Card Association (Visa, Master Card etc)
- Third party processor

Debit Card- The difference between credit cards and debit cards is that in order to pay with a debit card you need to know your personal identification number (PIN) and need a hardware device that is able to read the information that is stored in the magnetic strip on the back [3].

Debit cards task similar to checks in that the charges will be taken from the customer's checking account. The benefit for the customer is the easiness of use and convenience. These cards also keep the customer under his or her budget because they do not allow the customer to go beyond his or her resources. The advantage to the merchant is the speed at which the merchant collects these charges.

Smart Card- It was first introduced by Motorola, 1977. A smart card is a plastic card with an embedded microchip containing information about you. A smart card can store about 100 times the amount of information that a magnetic strip plastic card can store. A smart card contains private user information, such as financial facts, private encryption keys, account information, credit card numbers, health insurance information, etc. Popular in Europe, Germany, Singapore and Japan to pay for public phone call, transportation. Smart cards can accommodate a variety of applications that allow the customer to make purchases from a credit account, debit account, or stored value on the card.

These cards can even have multiple applications operating at the same time. The customer, for example, could have a frequent flyer program working on the same card as the customer debit or credit account. This enables the customer to earn points in his or her favorite program

Smart cards are of two types:

1. Relationship-based Smart Cards also called as Contact: It is the enhancement of existing card services that offer customers far better options like:

- Access to multiple accounts (debit, credit, e-cash) on one card.
- Offer various functions (cash access, bill payment, balance inquiry, fund transfer)
- Multiple access options at multiple location using multiple access device (ATM,

PC, PDA or screenphone etc)

2. Electronic Purses and Debit Cards also called as Contact-Less: Electronic Purses or E- wallet are the smart cards embedded with programmable microchip that store sum of money instead of cash. Once a purse is loaded with money it require card reader vending machine which verifies its authenticity .Then after amount is deducted from balance. It shows the remaining balance on the card hence eliminate the small bill in busy stores. E-wallets when depleted can be recharged with money.

E-Wallet- To facilitate the credit-card order process, many companies are introducing electronic wallet services. E-wallets allow you to keep track of your billing and shipping information so that it can be entered with one click at participating merchants' sites. E-wallets can also store echeques, e-cash and your credit-card information for multiple cards. A popular example of an e-wallet in the market is Microsoft Wallet. It can be used for micro-payments. They also eliminate

reentering personal information on the forms, resulting in higher speed and efficiency for online shoppers.

Micro payments-Micro-payments are used for small payments on the Web. The process is similar to e-wallet technology where the customer transfers some money into the wallet on his or her desktop and then pays for digital products by using this wallet. Using micro-payment one will be able to pay for one article from a professional journal, a chapter from a scientific book, or one song from a CD on the Web. There are many vendors involved in micro-payment systems. IBM offers micropayment wallets and servers. IBM micro-payment systems allow vendors and merchants to sell content, information, and services over the Web.

Automated Clearing House (ACH) routes bank transactions among financial institutions so that accounts held by respective financial institutions can be debited and credited.

VI. MAIN CONCERNS IN E-BANKING

In a survey conducted by the Online Banking Association, member institutions rated security as the most important issue of online banking. Unauthorized access or Phishing is one of the main risks in Internet Banking. If a customer provides his internet banking credentials in a website, that is not a legit bank website, his details can be used by the fake website to access his bank account and make transactions.

To control this - customers should be educated about phishing and asked to validate the authenticity of the website before they enter their credentials. In addition, customers must keep their credentials memorized and if they have written it down, they must keep it in a safe place that can be accessed only by them.

There is a dual requirement to protect customers' privacy and protect against fraud. Banking Securely: Online Banking via the World Wide Web provides an overview of Internet commerce and how one company handles secure banking for its financial institution clients and their customers. Some basic information on the transmission of confidential data is presented in Security and Encryption on the Web. PC Magazine Online also offers a primer: How Encryption Works. A multi-layered security architecture comprising firewalls, filtering routers, encryption and digital certification ensures that your account information is protected from unauthorized access:

- Firewalls and filtering routers ensure that only the legitimate Internet users are allowed to access the system.
- Encryption techniques used by the bank (including the sophisticated public key encryption) would ensure that privacy of data flowing between the browser and the Infinity system is protected.
- Digital certification procedures provide the assurance that the data you receive is from the Infinity system.

Security Solution

- A multi-layered security architecture comprising firewalls, filtering routers, encryption and digital

certification ensures that your account information is protected from unauthorized access

- Firewalls and filtering routers ensure that only the legitimate Internet users are allowed to access the system.
- Encryption techniques used by the bank (including the sophisticated public key encryption) would ensure that privacy of data flowing between the browser and the Infinity system is protected.
- Digital certification procedures provide the assurance that the data you receive is from the Infinity system.

Disadvantage

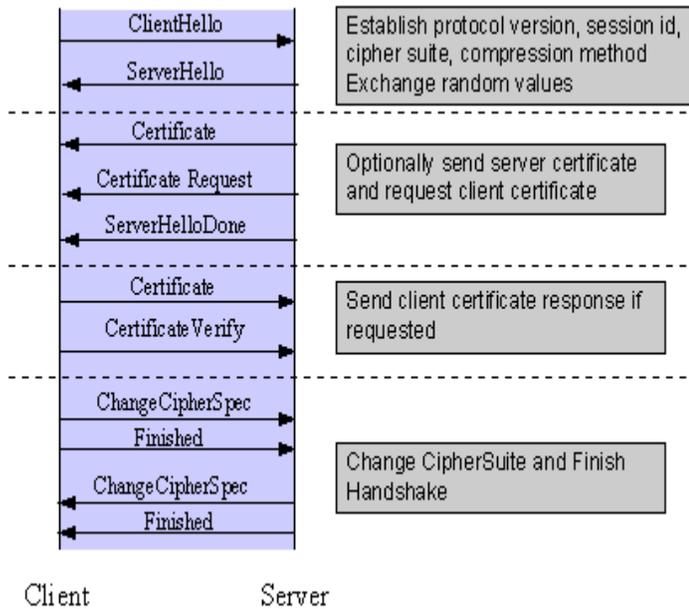
- Distorted facts are possible with such a plethora of information. Investors looking for information may find the wrong information or information that has been cooked, changed, or distorted in the corporations' favor.
- Also, the more information there is out there, the harder it is to find the information you need because you have to trudge through all the excessive information

Secure Sockets Layer (SSL) is a protocol developed by Netscape Communications Corporation. It provides secure communications over an open communication network, like the Internet. SSL provides data privacy and integrity as well as server and client authentication.

Once the server has a digital certificate, SSL-enabled browsers like Microsoft Internet Explorer can communicate securely with the server using SSL. With SSL, one can easily establish a security-enabled Web site on the private intranet or on the Internet.

SSL uses a security handshake to initiate a secure connection between the client and the server. During the handshake, the client and server agree on the security keys they will use for the session and the algorithms they will use for encryption. The client authenticates the server; optionally, the server can request the client's certificate.

Establishing a Session:



After the handshake, SSL is used to encrypt and decrypt all of the information in both the https request and the server response, including:

- The URL the client is requesting.
- The contents of any form being submitted.
- Access authorization information like user names and passwords.
- All data sent between the client and the server.

SSL defines methods for data encryption, server authentication, message integrity, and client authentication for a TCP/IP connection. SSL uses public key and symmetric techniques to protect information.

HTTPS is a unique protocol that combines SSL and HTTP. A client user can open a URL by specifying https:// to request an SSL-protected documents. HTTPS (HTTP + SSL) and HTTP are different protocols and use different ports (443 and 80, respectively), you can run both SSL and non-SSL requests at the same time. As a result, you can choose to provide information to all users using no security, and specific information only to browsers who make secure requests.

On the internet, **HTTPS** provides authentication of the web site and associated web server that one is communicating with, which protects against Man-in-the-middle attacks. Additionally, it provides bidirectional encryption of communications between a client and server, which protects against eavesdropping and tampering with and/or forging the contents of the communication. In practice, this provides a reasonable guarantee that one is communicating with precisely the web site that one intended to communicate with (as opposed to an impostor), as well as ensuring that the contents of communications between the user and site cannot be read or forged by any third party.

Because HTTPS piggybacks HTTP entirely on top of TLS, the entirety of the underlying HTTP protocol can be encrypted. This includes the request URL (which particular web page was requested), query parameters, headers, and cookies

(which often contain identity information about the user). However, because host (web site) addresses and port numbers are necessarily part of the underlying TCP/IP protocols, HTTPS cannot protect their disclosure. In practice this means that even on a correctly configured web server eavesdroppers can still infer the IP address and port number of the web server (sometimes even the domain name e.g. www.example.org, but not the rest of the URL) that one is communicating with as well as the amount (data transferred) and duration (length of session) of the communication, though not the content of the communication.

Historically, HTTPS connections were primarily used for payment transactions on the World Wide Web, e-mail and for sensitive transactions in corporate information systems. In the late 2000s and early 2010s, HTTPS began to see widespread use for protecting page authenticity on all types of websites, securing accounts and keeping user communications, identity and web browsing private.

The SET (Secure Electronic Transaction) standard is a global industry specification that was developed jointly by Visa International, MasterCard, and other companies. The SET protocol uses digital certificates to protect credit card transactions that are conducted over the Internet. The SET standard is a major step toward securing Internet transactions, paving the way for more merchants, financial institutions, and consumers to participate in electronic commerce. ICSF provides callable services that support the development of SET applications that run at the merchant and acquirer payment gateway.

SET addresses seven major business requirements:¹

1. Provide confidentiality of payment information and enable confidentiality of order information that is transmitted along with the payment information.
2. Ensure the integrity of all transmitted data.
3. Provide authentication that a cardholder is a legitimate user of a branded payment card account.
4. Provide authentication that a merchant can accept branded payment card transactions through its relationship with an acquiring financial institution.
5. Ensure the use of the best security practices and system design techniques to protect all legitimate parties in an electronic commerce transaction.
6. Create a protocol that neither depends on transport security mechanisms nor prevents their use.
7. Facilitate and encourage interoperability among software and network providers.

Point 1 ensures that card information cannot be viewed by unauthorized parties. Point 2 ensures that the information cannot be changed or tampered. Points 3 and 4 ensure that the cardholder and merchant are really who they claim they are. Hence, in essence, this framework, if implemented effectively, will allow both buyers and sellers to transact in total confidence in an open network.

VII. E-BANKING CASE STUDY

Intuit: Intuit is a leading provider of financial software it pioneered the concept of e-banking by making a personal finance software called Quicken in 1984. It launched online bill payment services in the year 1990, IntelliCharge credit card service in 1993 and Quicken Quotes a portfolio price update service in 1994.

At the forefront was the company's software Quicken; it allows users to organize, understand and manage their personal finance. Quicken looks and works like a chequebook, it allows users to enter their financial transactions and then generate meaningful reports and graphs. It allows users to reconcile their bank accounts and also track their credit card purchases. It also enables users to print cheques from the computer and allows them to make online payments.

The company also offers to its customer's online banking, bill payment and credit management.

How It Works:

Customers will have to sign up with a local bank and then use Quicken software to get the desired information. Quicken users then dial a local number and all transactions between Quicken and the banks are done through an Intuit subsidiary National Payment Clearing House, which changed its name to Intuit Service Corporation. ISC is an intermediary between the Quicken software and the banks. ISC's network design is based on "burst and disconnect" i.e. the user connects to ISC gets his desired information and disconnects. This strategy allows full utilization of the network and allows maximum number of users. The network applies the RSA security method. Intuit is banking partners download all bank related information like bank balances and statements into ISC's servers. So that all information is available to the user from his computer and modem. In case of credit card payments, the request is passed to the credit card company, which feeds the details about the latest transactions to ISC, which then gets back to the user.

In case of Bill Payment, the user just logs into the ISC server and feeds the details of the bills he has to pay. ISC then sees the most appropriate method of payment of the bill. There may be many possible ways, as some companies may have tied up with ISC itself, some may have tied up with other networks etc. If the bill cannot be paid over the network then Intuit prints a physical cheque and sends it to the party.

VIII. CONCLUSION

The online payment system facilitates the acceptance of electronic payment for online transactions, in other words, enables monetary value to be transferred digitally. The e-commerce payment systems have become increasingly popular due to the widespread use of the internet-based shopping and banking.

Traditional payment methods include cash, cheque, credit and debit cards. The problems with the traditional ways are inconvenience, lack of security, coverage & the time involved in the process etc. Over which the e-banking offers facilities at lower costs, convenience to the customers in varied domains like

paying utility bills, taxes etc and overall reducing the time involved in process.

The paper discusses the internet based payment models like EFT, payment cards, credit cards, smart cards, e-money, micro-payment systems, electronic wallets etc.

The risks to the use of e-commerce are identity theft & theft of payment data, & fraudulent rejection of the part of consumers. Security is considered to be most important issue of online banking. To control unauthorized access & phishing the customers should be educated about these threats and ways to prevent these.

With respect to the payment methods that have been discussed here, it is impossible to say that any one of them is perfect, although each one of them has advantages opposed to the others. A multi-layered security architecture comprising firewalls, filtering routers, encryption and digital certification ensures that users' information is protected. Therefore and until the use of electronic signature is wide spread, we must use the technology available for the moment to guarantee a reasonable minimum level of security on the network.

REFERENCES

- [1] Akudo C. Anyanwu, Absalom E. Ezugwu, Sale E. Abdullahi , "Electronic Payment System (EPS):Facilitating the Development and Adoption in Nigeria", IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 2, No 1, March 2012
- [2] Awad, E.M. Electronic Commerce from vision to Fulfillment. Pearson Education. 2007
- [3] Chhabra, T.N. Suri, R.K. & Verma, S. e-commerce new vistas for Business.Dhanpat Rai & Co. 2007-2008
- [4] Kalakota & Winston. Frontiers of Electronic Commerce. Pearson Education, LPE. 2003
- [5] Jaiswal, S. Doing business on the Internet E-Commerce. Galgotia publication Pvt. Ltd. 2003
- [6] http://httpd.apache.org/docs/2.2/ssl/ssl_intro.html
- [7] <https://www.cibc.com/ca/student-life/banking-101/intro-to-banking/benefit-online-bnkg.html>
- [8] http://en.wikipedia.org/wiki/HTTP_Secure
- [9] <http://www.informedia.cs.cmu.edu/documents/netbill.pdf>
- [10] <http://www.isaca.org/Journal/Past-Issues/2000/Volume-6/Pages/Secure-Electronic-Transaction-SET-Protocol.aspx>
- [11] <http://www.moneymatters101.com/banking/onbk.asp>
- [12] http://ocw.metu.edu.tr/pluginfile.php/354/mod_resource/content/0/Lecture_4.pdf
- [13] <http://online-only-banks-review.toptenreviews.com/online-banking-vs.-traditional-banking.html>
- [14] <http://publib.boulder.ibm.com/infocenter/zos/v1r11/index.jsp?topic=/com.ibm.zos.r11.halz002/encalg.htm>
- [15] <http://rbidocs.rbi.org.in/rdocs/Publications/PDFs/4456.pdf>
- [16] <http://www.sis.pitt.edu/~spring/E-Business/example/pdf/FinancialSupport.PDF>
- [17] <http://webserver.ignou.ac.in/virtualcampus/adit/course/cst304/ecom2.htm>

AUTHORS

First Author – Mukta Sharma, Research Scholar, TMU, m.mukta19@gmail.com

Second Author – Dr. R.B. Garg , HOD CS/MCA, Tecnia, IP University, Ex-Prof., Delhi University, garg1943@gmail.com

