

Payment Processing Systems and Security for E-Commerce: A Literature Review

Ms. Vaishnavi.J.Deshmukh¹

Lecture Computer Engg Department
SGBAU-Amravati University
India.

Sapna.S.Kaushik²

Lecturer Computer Engg Department
SGBAU-Amravati University
India.

Mr. Amit.M.Tayade³

Lecturer Computer Engg Department
SGBAU-Amravati University
India.

Abstract— *Electronic Commerce is process of doing business through computer networks. A person sitting on his chair in front of a computer can access all the facilities of the Internet to buy or sell the products. Unlike traditional commerce that is carried out physically with effort of a person to go & get products, ecommerce has made it easier for human to reduce physical work and to save time. E-Commerce which was started in early 1990's has taken a great leap in the world of computers, but the fact that has hindered the growth of e-commerce is security. Security is the challenge facing e-commerce today & there is still a lot of advancement made in the field of security. The main advantage of e-commerce over traditional commerce is the user can browse online shops, compare prices and order merchandise sitting at home on their computers. For a developing country advancement in the field of e-commerce is essential. The research strategy shows the importance of the e-commerce in developing countries for business applications. Electronic commerce or ecommerce is a term for any type of business, or commercial transaction, that involves the transfer of information across the Internet. It covers a range of different types of businesses, from consumer based retail sites, through auction or music sites, to business exchanges trading goods and services between corporations. It is currently one of the most important aspects of the Internet to emerge.*

Keywords— *E-commerce, B2B, B2C C2C, Electronic Payment- EPS, ACH, EFT, SET, SSL, IOTP*

I. INTRODUCTION

Electronic payment systems are central to on-line business process as companies look for ways to serve customers faster and at lower cost. Emerging innovations in the payment for goods and services in electronic commerce promise to offer a wide range of new business opportunities. Electronic payment systems and e-commerce are highly linked given that on-line consumers must pay for products and services. Clearly, payment is an integral part of the mercantile process and prompt payment is crucial. If the claims and debits of the various participants (consumers, companies and banks) are not balanced because of payment delay, then the entire business chain is disrupted. Hence an important aspect of e-commerce is prompt and secure payment, clearing, and settlement of credit or debit claims. To circumvent some of these problems, traders invented various forms of payment instruments. The merchants also developed commercial law surrounding the use of these instruments that proved to be one of the turning points in the history of trade and commerce. We are on the verge of a similar sort of development today, but one that is unlikely to take anywhere near the centuries it took for the traditional payment system to evolve. Everyone agrees that the payment and settlement process is a potential bottleneck in the fast-moving electronic commerce environment if we rely on conventional payment methods such as cash, checks, bank drafts, or bills of exchange. Electronic replicas of these conventional instruments are not well suited for the speed required in e-commerce purchase processing. For instance, payments of small denominations (micropayments) must be made and accepted by vendors in real time for snippets of information. Conventional instruments are too slow for micropayments and the high transaction costs involved in processing them add greatly to the overhead. Therefore new methods of payment are needed to meet the emerging demands of e-commerce. These neo-payment instruments must be secure, have a low processing cost, and be accepted widely as global currency tender.

II. E-COMMERCE

An easy way to comply with the conference paper formatting requirements is to use this document as a template and simply type your text into it.

A. Features of E-Commerce Technology

Electronic business can result in better transactions, wide market coverage by offering the benefits of speed, convenience, being cost effective, timeliness, high profit margins, instant customer relations, no loss of customers, impact and control- all are a fraction of the past traditional business methods. A business will always have the information it needs faster, easier and more completely in the new system of communication than ever before.

- **Improve Responsiveness-** It helps by improving responsiveness to market conditions and customer preferences. Every business must know how important timing is to marketing and selling products. Timing is important to cater to the demands of customers. If distributors, dealers and sales force do not get the right information at the right time, there will be a financial crisis as well as losing valuable customers. E-commerce network enables a company to implement marketing programs with greater precision such as Pre-empt competitiveness with a change in marketing tactics before they can react. Improve responsiveness by revising price change and marketing programs as and when required.

• Close Contact with Clients- In any business where maintaining close contact with customers is a priority consideration, electronic business can increase responsiveness of the company' and ensure customer satisfaction. Appointment confirmations, requests for information, follow-up reports and electronic data interchange can be effected with greater efficiency using instant messages.

B. Levels of E-Commerce

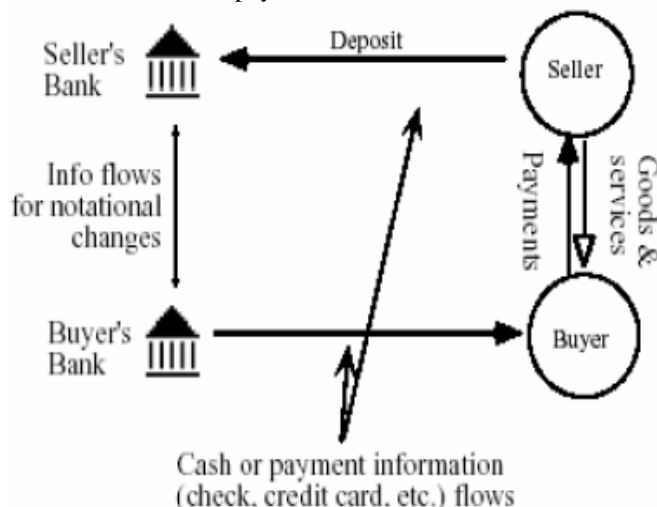
Electronic commerce is the process of conducting commercial transactions electronically over the Internet. This process is carried out primarily in five levels, and the main aspect of e-commerce is a merchant selling products or service to the consumers. There are five major segments under the broader category of e-business. However, the following are some popular e-commerce models used by companies engaged in e-commerce:-

- Business to business e-commerce (B2B)
- Business to consumers e-commerce (B2C)
- Consumers to consumers e-commerce (C2C)
- Business to employees e-commerce (B2E) and
- Consumer to business e-commerce (C2B)

III. TYPES OF ELECTRONIC PAYMENT SYSTEM

Electronic payment systems are becoming central to on-line business transactions nowadays as companies look for various methods to serve customers faster and more cost effectively. Electronic commerce brings a wide range of new worldwide business opportunities.

A conventional process of payment and settlement involves a buyer-to-seller transfer of cash or payment information (e.g. credit card or check). The actual settlement of payment takes place in the financial processing network. A cash payment requires a buyer's withdrawal from his bank account, a transfer of cash to the seller, and the seller's deposit of the payment to his/her account. Non-cash payment mechanisms are settled by adjusting, i.e. crediting and debiting, the appropriate accounts between the banks based on payment information conveyed via check or credit card. Figure 1. is a simplified diagram for both cash and non-cash transactions. If a buyer uses a non-cash method of payment, payment information instead of cash flows from the buyer to the seller, and ultimately payments are settled between affected banks who notationally adjust accounts based on the payment information..



. Fig. 1. A Cheque simplified model of transaction as a function of applied field.

A. Payment through an Intermediary - Payment Clearing Services

When face-to-face purchase is replaced with on-line commerce, many aspects of a transaction occur instantly, under which various processes of a normal business interaction are subsumed. For example, a typical purchase involves stages of locating a seller, selecting a product, asking a price quote, making an offer, agreeing over payment means, checking the identity and validity of the payment mechanism, transferring of goods and receipts. In order to be used as a substitute for face-to-face payments, online payment systems must incorporate all or some of these stages within their payment functions. The lack of face-to-face interaction also leads to more secure methods of payment being developed for electronic commerce, to deal with the security problems for sensitive information and uncertainty about identity. Consequently, electronic commerce transactions require intermediaries to provide security, identification, and authentication as well as payment support.

Figure .2 shows a stylized transaction for online commerce using an intermediary. In this model, the intermediary not only settles payments, it also takes care of such needs as confirming seller and buyer identities, authenticating and verifying ordering and payment information and other transactional requirements lacking in virtual interactions. In the figure, two boxes delineate online purchasing and secure or off-line payment clearing processes. Payment settlement in

this figure follows the example of the traditional electronic funds transfer model which uses secured private value networks. The intermediary contributes to market efficiency by resolving uncertainties about security and identity and relieving vendors of the need to set up duplicative hardware and software to handle the online payment clearing process.

The key benefit of this payment clearing system is that it separates sensitive and non-sensitive information and only non-sensitive information is exchanged online. This alleviates the concern with security that is often seen as a serious barrier to online commerce. In fact, First Virtual does not even rely on encryption for messages between buyers and sellers. A critical requisite for this system to work is the users' trust in the intermediaries.

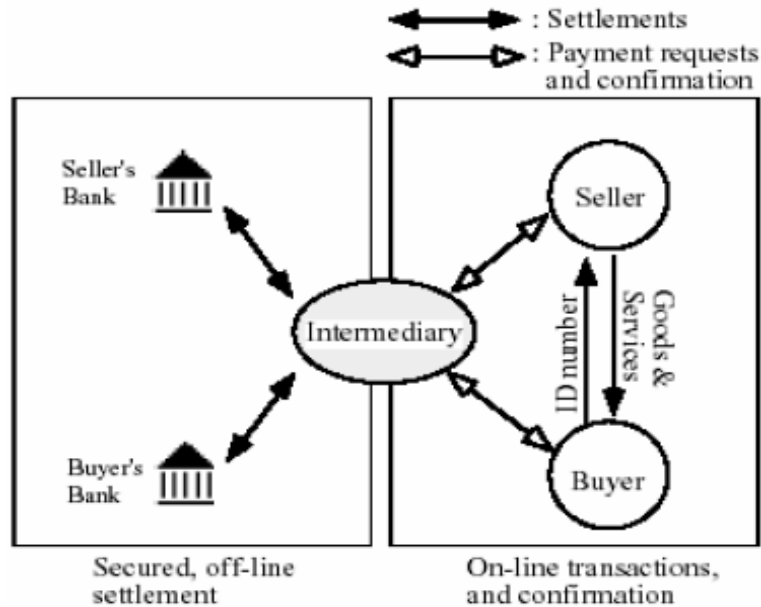


Fig. 2. Transactions with an intermediary.

B. Payment Based on EFT - Notational Funds Transfer

The second type of payment systems does not depend on a central processing intermediary. Instead, sensitive payment information (such as credit card or bank account number) is transmitted along with orders, which is in effect an open Internet implementation of financial electronic data interchange (EDI) (see Figure .3). An electronic funds transfer (EFT) is a financial application of EDI, which sends credit card numbers or electronic checks via secured private networks between banks and major corporations. To use EFTs to clear payments and settle accounts, an online payment service will need to add capabilities to process orders, accounts and receipts. In its simplest form, payment systems may use digital checks —simply an image of a check— and rely on existing payment clearing networks. The Secure Electronic Transaction (SET) protocol - a credit card based system supported by Visa and MasterCard - uses digital certificates, which are digital credit cards.

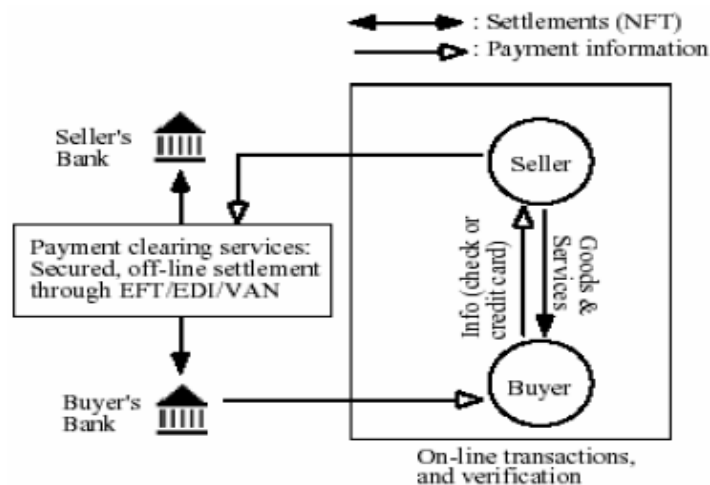


Fig. 3. A Notational funds transfer system.

Notational funds transfer systems differ from payment clearing services in that the 'payment information' transferred online contains sensitive financial information. Thus, if it is intercepted by a third party, it may be abused like stolen credit cards or debit cards. A majority of proposed electronic payment systems fall into this second type of payment systems. The objective of these systems is to extend the benefit and convenience of EFT to consumers and small businesses. However, unlike EFTs, the Internet is open and not as secure as private value added networks (VANs). The challenge to these systems is how to secure the integrity of the payment messages being transmitted and to ensure the interoperability between different sets of payment protocols.

C. Payment Based on Electronic Currency

The third type of payment systems transmit not payment information but a digital product representing values: electronic currency. The nature of digital currency mirrors that of paper money as a means of payment. As such, digital currency payment systems have the same advantages as paper currency payment, namely anonymity and convenience. As in other electronic payment systems, here too security during transmission and storage is a concern, although from a different perspective, for digital currency systems doubling, counterfeiting, and storage become critical issues whereas eavesdropping and the issue of liability (when charges are made without authorization) are important for notational funds transfers. Figure 4 shows a digital currency payment scheme. The only difference from Figure is that the intermediary in Figure 4. acts as an electronic bank which converts outside money, into inside money (e.g. tokens or e-cash) which is circulated within online markets.

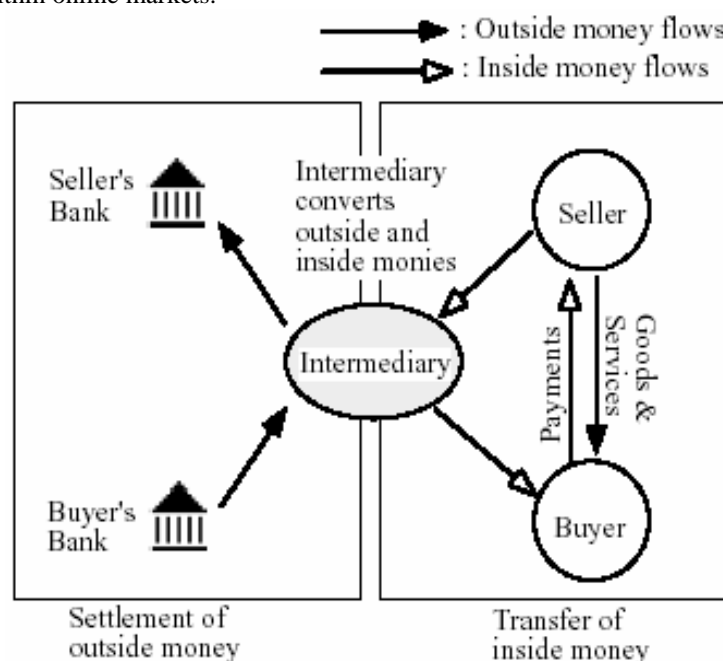


Fig. 4. A Digital Currency Payment Scheme.

IV. ELECTRONIC PAYMENT PROTOCOLS

There are many protocols that are currently employed to allow money to change hands in cyberspace. But the most important open protocols used for payments on the Web are SSL/TLS, SET, and IOTP.

A. SSL and TLS Protocol

The Secure Sockets Layer (SSL) protocol was designed by Netscape as a method for secure client-server communications over the Internet. Using public key cryptography and certificates, SSL offers a mechanism so that clients and servers can authenticate each other and then engage in secure communication. During an initial handshaking phase, the client and server select a secret key crypto scheme to use and then the client sends the secret key to the server using the server's public key from the server's certificate. From that point on, the information exchanged between the client and server is encrypted. SSL/TLS is an intermediate protocol layer that sits between TCP and a higher-layer application. SSL/TLS can be employed by any application layer protocol running over the Transmission Control Protocol (TCP), including Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP),

As the SSL/TLS protocol handshaking in Figure 5 shows, however, the protocol provides the messages and procedures so that a certificate could be provided by both client and server. TLS continues the evolution started by SSL. Market acceptance and user confidence in the protocol is extremely high and its use will clearly continue. It is worth noting that SSL/TLS is sufficiently secure for the vast majority of consumers who use it today to guard everything from credit card transactions and electronic banking to voting their proxy shares and applying to college.

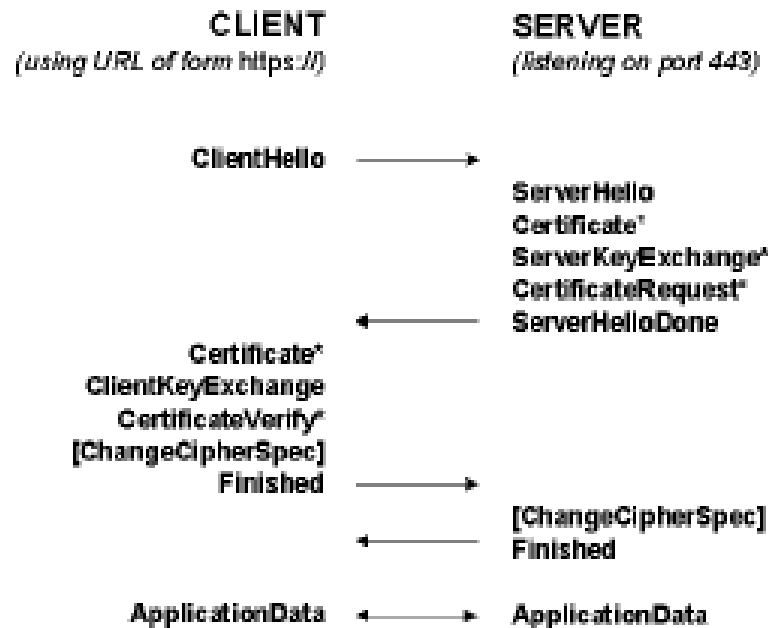


Fig. 5. SSL/TLS messages exchanged between client and server.

B. Secure Electronic Transaction Protocol (SET)

The Secure Electronic Transaction (SET) protocol specifically handles electronic payments. Fraud prevention is a primary motivator behind SET. That would seem to indicate that the current model of using SSL to protect transactions is adequate. SET has the potential to reduce the chance of fraud by providing rigorous authentication measures in addition to encrypting transactions.

SET provides a high degree of privacy for customers by encrypting payment information so that only the bank can see it. Customer software sends a purchase request to the merchant containing the following Figure 6, unencrypted order information and a dual signature, intended for the merchant; payment instructions and a dual signature, both encrypted and intended for the payment gateway; and the cardholder's digital certificate to be used by the merchant and the payment gateway for authentication.



Fig. 6. SET Purchase Request.

C. Internet Open Trading Protocol (IOTP)

The Internet Open Trading Protocol (IOTP) provides an interoperable framework for consumer-to-business Internet-based electronic commerce. As a commerce framework specification, IOTP is designed to replicate the "real" world of transactions where consumers choose their product, choose their vendor, choose their form of payment (in conjunction with their vendor), arrange delivery, and, periodically, even return products. The designers of IOTP intend that this protocol will be the lingua franca of Internet commerce just as EDI has become the standard document language for "real" commerce; any two parties conducting Internet-based e-commerce in a way that conforms to the IOTP specifications will be able to complete their transactions securely.

Figure 7 shows the general flow of an IOTP-based purchase. Note that it might be more proper to refer to IOTP as a shopping protocol rather than a payment protocol since it attempts to capture the entire online shopping cycle and shopping is more than merely paying for stuff. And just as you might wander through the stores of a new mall in the real world, IOTP is optimized for those cases where the buyer and merchant do not have an a priori relationship.

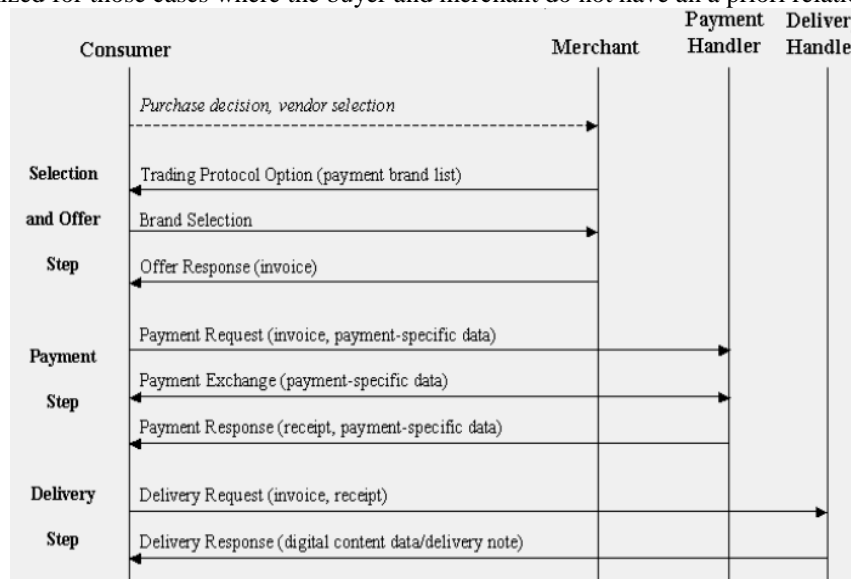


Fig. 7. Flow of IOTP

V. SECURITY REQUIREMENTS IN ELECTRONIC PAYMENT SYSTEM

The concrete security requirements of electronic payment systems vary, depending both on their features and the trust assumptions placed on their operation. In general, however, electronic payment systems must exhibit integrity, authorization, confidentiality, availability, and reliability.

A. Integrity and Authorization

A payment system with integrity allows no money to be taken from a user without explicit authorization by that user. It may also disallow the receipt of payment without explicit consent, to prevent occurrences of things like unsolicited bribery. Authorization constitutes the most important relationship in a payment system. Payment can be authorized in three ways: via out-band authorization, passwords, and signature.

B. Out-band Authorization

In this approach, the verifying party (typically a bank) notifies the authorizing party (the payer) of a transaction. The authorizing party is required to approve or deny the payment using a secure, out-band channel (such as via surface mail or the phone). This is the current approach for credit cards involving mail orders and telephone orders: Anyone who knows a user's credit card data can initiate transactions, and the legitimate user must check the statement and actively complain about unauthorized transactions. If the user does not complain within a certain time (usually 90 days), the transaction is considered "approved" by default.

C. Password Authorization

A transaction protected by a password requires that every message from the authorizing party include a cryptographic check value. The check value is computed using a secret known only to the authorizing and verifying parties. This secret can be a personal identification number, a password, or any form of shared secret. In addition, shared secrets that are short - like a six-digit PIN - are inherently susceptible to various kinds of attacks. They should only be used to control access to a physical token like a smart card (or a wallet) that performs the actual authorization using secure cryptographic mechanisms, such as digital signatures.

D. Signature Authorization

In this type of transaction, the verifying party requires a digital signature of the authorizing party. Digital signatures provide nonrepudiation of origin: Only the owner of the secret signing key can "sign" messages (whereas everybody who knows the corresponding public verification key can verify the authenticity of signatures.)

E. Confidentiality

Some parties involved may wish confidentiality of transactions. Confidentiality in this context means the restriction of the knowledge about various pieces of information related to a transaction: the identity of payer/payee, purchase content, amount, and so on. The confidentiality requirement dictates that this information be restricted only to the participants involved. Where anonymity or un-traceability are desired, the requirement may be to limit this knowledge to certain subsets of the participants only, as described later.

F. Availability and Reliability

All parties require the ability to make or receive payments whenever necessary. Payment transactions must be atomic: They occur entirely or not at all, but they never hang in an unknown or inconsistent state. No payer would accept a loss of money (not a significant amount, in any case) due to a network or system crash. Availability and reliability presume that the underlying networking services and all software and hardware components are sufficiently dependable

VI. ELECTRONIC PAYMENT SYSTEM IN INDIA

These are Safety, Security, Soundness and Efficiency. Called the 'Triple-S + E' principle in short, each of the principles, which have a synergistic inter-relationship, would specifically address the following:

- Safety will relate to addressing risk, so as to make the systems risk free or with minimal risk.
- Security will address the issues relating to confidence, with specific reference to the users of these systems.
- Soundness will be aimed at ensuring that the systems are built on strong edifices and that they stand the test of time.
- Efficiency will represent the measures aimed at efficiencies in terms of costs so as to provide optimal and cost effective solutions.

There are a few large value payment systems functioning in the country. These are the Inter-Bank Cheques Clearing Systems (the Inter-bank Clearing), the High Value Cheques Clearing System (the High Value Clearing), the Government Securities Clearing System (the G-Sec Clearing), the Foreign Exchange Clearing System (the Forex Clearing) 15 places - both are managed by the Reserve Bank. The G-Sec Clearing and the Forex Clearing are managed by the Clearing Corporation of India Limited (CCIL). The RTGS System is operated by the Reserve Bank. All these are deemed to be Systemically Important Payment Systems (SIPS) and therefore the Reserve Bank has, in line with the international best practices in this regard, moved them (except the Inter-bank Clearings at places other than Mumbai and the High Value Clearings) to either secure and guaranteed systems or the RTGS System

VII. CONCLUSIONS

Although there is a plethora of disparate payment systems offered for electronic commerce, many firms are reluctant to expand into online commerce because of the perceived lack of suitable payment mechanisms. Widely different technical specifications make it difficult to choose an appropriate payment method. In our paper, instead of focusing on the technical specifications of proposed electronic payment systems, we have distinguished electronic payment methods based on what is being transmitted over the network. Since consumers are familiar with credit card payment methods, they may accept its electronic versions as the standard for electronic commerce. Factors such as micropayments and peer-to-peer currency in electronic commerce-especially for the information market-seem to indicate a healthy market for digital currency or small-value digital checks or credit cards. In terms of the regulatory and monetary impact, private digital monies clearly present both problems and opportunities. But, as with any digital product, the future of digital currency will be determined by the market demand and supply. Consequently, it is more than likely that each of the payment methods we reviewed will find a niche market and consumers will selectively use an appropriate payment method depending on whether one prefers convenience, costs, privacy, or the advantage of credit extension. With a suitable payment method, the age of information will manifest itself on the Internet, albeit in a commercial form

ACKNOWLEDGMENT

I acknowledge our senior faculty who has provided us their views in the selection of topic. Also I am thankful to my Department for the technical support.

REFERENCES

- [1] Kalakota, Ravi and Whinston, Andrew B. "Electronic Commerce – A Manager's Guide", Pearson Education, Inc..
- [2] Kalakota, Ravi and Whinston, Andrew B. "Frontiers of Electronic Commerce", Pearson Education, Inc.
- [3] Rich, Jason R. "Starting an E-Commerce Business". IDG Books, Delhi, 2000.
- [4] Samantha Shurety. "E-business with Net Commerce", Addison Wesley, Singapore, 2001.
- [5] Turban et al. "Electronic Commerce: A Managerial Perspective", Pearson Education, Inc.



Vaishnavi J Deshmukh, 3 June'1989 , received her bachelor's degree in Computer Science & Engineering from Amravati University. She is currently working as an assistant professor with the Department of Computer Engineering, D.B.N.C.O.E.T, SGBAU-Amravati University, India.

Her research interests mainly focused on E-Commerce , Mobile ad Hoc Networks, Network Security.