CHAPTER 2

E-BANKING: A CONCEPTUAL FRAMEWORK

I. Review of Literature
II. Conceptual Framework of E-Banking
III. Security in E-Banking
IV. Working of payment gateways
V. e-fraud cases
VI. e-fraud and online banking protection
VII. Conclusion

1 Review of Literature:

2.1.1 Introduction:

Review of literature is concerned to the study of previous research work in the field of chosen research problem and other problems related to E-banking services. This is one of the most important components in the research process, which introduces research gaps as well as the research process to researchers. It also provides the researcher a bird’s eye view about the research done in that area so far. In order to get acquaintance with the research process, to understand the research gaps in the chosen research study, earlier research articles, published proceedings in national and international conferences, references where reviewed.

The presentation of review of literature is grouped under the following headings:

2.1.2 Review from national and international journals.

2.1.3 Review from reference books.

2.1.4 Review from committees.

2.1.5 Review from conferences.

2.1.6 Review from Ph.D. thesis.
2.1.2 Review from National and International Journals:

Parasuraman, Zeithaml and Berry (1985) they defined service quality as the gap between the customers perceptions and expections of service performance. Based on this conceptualizations and operationalization, they proposed a service quality measurement scale called SERVQUAL. The SERVQUAL instrument identifies service quality from the customer’s perspective. After clearing the gaps and on the basis of the work done by Fitzsimmons and Fitzsimmons (1990), they have identified five dimensions with which consumers judge service quality. The literature has been extensively applied in different series settings. It is basically a multi-item scale used for measuring the five dimensions of service quality (i.e. Reliability, Responsiveness, Assurance, Empathy and Tangibility) each dimension containing multiple items that measures the organizations strengths and weaknesses in the area of service quality. SERVQUAL can also be used for comparing service to identify the criteria for superior service quality.[1]

Bhattacharya (1997) he has studied the impact of the limited liberalization initiated before the deregulations of the 90’s on the performance of the different categories of banks. His study covers 70 banks in the period 1986-91. He has constructed one grand frontier for the entire period and measured technical efficiency among the three categories with foreign and private banks having much lower efficiencies. The main results accord with the general perception that in the nationalized era, public sector banks were successful in achieving their principle objectives of deposit and loan expansion.[2]

Kangis and Vouklatos (1997) their objectives of the research are to compare the customers expectations and perceptions of service quality (SQ) in public and private sector banks. For study purpose, 163 bank customers were selected and used pre-tested questionnaire containing 12 service quality items of SERVQUAL. Correlation technique was used for analysis of data. Findings of the study is that customers of private sector banks were found to have lower level of difference between perception and expectations of SQ than the customers of public sector bank. Convenient location, operating hours, friendliness and courtesy of employees were not considered as important factors by the customers of both sector banks.[3]

Joseph et.al. (1998) investigated the role of technology on Australian banking sector. In sample size, 68 bank customers were surveyed through 22 items of SERVPERF scale. Ordinary Least Square (OLS) and Factor Analysis techniques are used. It is found that technical/functional quality model was better than SERVQUAL because later was lacking
technical dimensions. These two models have distinct and unique strengths for measuring SQ aspects. SQ and the type of communication influence customer satisfaction.[4]

Bhat and Gani (2003) compared the customers’ expectations and perceptions regarding SQ in public sector, private sector and foreign banks. 800 customers (50% -Public, 25% -Private and 25% -Foreign) and SERVQUAL was used. Mean difference and t-test was used for analysis. It is found that foreign banks were providing better quality services than Indian banks as they were supported by advanced technologies. Indian banks were far behind as far as the physical facilities and up-to-date equipment were concerned. Only PNB and J&K bank were providing the SQ which was somewhat near to the SQ provided by foreign banks to the customers.[5]

Hundal and Jain (2006) studied adoption of mobile banking services in India. The data was collected in India during 2005. The article articulates the stimulating and inhibiting attributes on the adoption of mobile banking services and outlines managerial implications.[6]

Sharma et. al. (2007) examined and compared the perceptions of customers regarding SQ in public and private sector banks. Structured questionnaire was prepared and 500 customers (400 from SBI and 100 from HDFC) have been selected. Percentage and weighted average scores were used for data analysis. It is found that SQ was positively associated with customer services and there was significant difference in the quality of services provided by selected banks. Banks located in small cities and towns were lagging behind their counterparts in big and metropolitans cities. [7]

Migdadi (2008) attempted to identify the service quality between Jorden and UK. The evaluation of the banks web sites was conducted in March 2008 for 16 click-and-morter retail banks in the UK and 6 dot com retail banks in UK. Result indicated that, the internet banking service encounter quality of the click-and-morter in Jorden, retail banks is very closed to the UK banks. Further quality of internet banking service encounter quality of the click-and-morter retail banks in the UK which are very close to the dot com and retail banks in the UK.[8]

Wong et. al. (2008) made a study to re-examine the role of traditional SQ in E-banking era in Australia. 706 customers and a self-administered questionnaire (22 items to measure SQ) was used for data collection. Quadrant analysis and Factor analysis techniques were used. They concluded that electronic delivery of services continuously increased the customers’ expectations of SQ and performance; where as traditional banking services was misaligned to their current expectations and it caused dissatisfaction. [9]
Rod et. al. (2009) examined the relationship between SQ, overall internet banking SQ and customer services in New Zealand banking sector. They selected 72 customers of national bank and collected opinion, using questionnaire (15 items to measure SQ). Data analysis was done through Soft Modeling SEM methodology, Partial Least Square (PLS). They pointed out that online customer SQ and online information systems were significantly and positively related to overall internet banking SQ. Overall internet banking SQ and customer services were positively associated.[10]

Riquelme et.al. (2009) studied the impact of customer services and online internet banking services attributes on overall satisfaction of bank customers in Kuwait. They selected 185 customers and collected response using questionnaire. Statistical tools like cross tabulations, multiple regression and discriminate analysis were used for data processing. They reported that 84.4% customers were found to be satisfied from online service but still using multiple channels to conduct transactions. Both customers and online service attributes were found to have significant impact on customer satisfaction. It is found that female customers are less satisfied with the way, the complaint are handled. Further least educated customers use ATMs less frequently.[11]

Gupta P K (2008) attempted to examine the customer’s behaviors with respect to internet banking vis-à-vis conventional banking. From major cities 2000 customers were selected and collected opinion through questionnaire. Statistical techniques such as percentages, F-ratios, cluster trees and factor analysis techniques were used. He concluded that, internet banking was found to be easier and speedier than conventional banking and trust was found as most important factor followed by accuracy and confidentiality. But on safety level, the rating in case of conventional banking system was found to rise with the movement to higher income levels.[12]

Khan et. al. (2009) their objective was to evaluate the SQ of internet banking services from the customers view point in India . To measure customer satisfaction, 1143 customers (700 from public sector, 330 from private and 113 from foreign banks) were surveyed through structured questionnaire containing 20 variables . Factor analysis, correlation regression, t-test techniques were used for analysis purpose. They observed that, customers are found to be satisfied with ‘reliability’ but dissatisfied with ‘user friendliness’. Two dimensions i.e. ‘privacy/security’ and ‘fulfillment’ were not significantly contributed towards overall SQ. High percentage of young generation having computer literacy, showed that internet banking was going to be very crucial in India. [13]
Mallya M D (2009) analyzed the role of IT in improving customer service. Bank customers can look forward to more exciting, innovative and technology-based products. Customers who can enjoy the use of computers can do most of the banking at home/office and experience the benefits of virtual banking. The emerging pattern of banking can help customers to manage their time better and banking can be an integral part of their routine activities. [14]

Dangwal, Kaur, Kapoor (2009) highlighted the significant effect of new economic policy of liberalization, privatization and globalization on the working of banks. In this paper the performance appraisal of new private sector banks has been measured through spread, burden and profitability ratios by considering eight parameters. They finally summarized, the spread and profitability ratios increased in new private sector banks in India during the period of study (i.e. March 2001-2005), also indicates that the performance of new private sector banks is on the incremental trend.[15]

Kumar and Saini (2009) studied the adoption of electronic banking technologies by Indian consumers. It has been observed in the findings that contextual and demographic variables influence the adoption of new technology in banking sector. Urban consumers are more confident than their rural counterparts in accepting the new technology. Further younger consumers reveal more openness to change and more familiar with the technology. Male consumers use technology more than the female and well educated consumers use technology more easily than those with lower educational status. Income has also been identified as an influence factor in the adoption of electronic technologies. Consumers from high income group use it more than the low income group.[16]

Sakthivel and Murugeshwari (2009) analyzed that, consumer have low level of awareness towards internet banking service of ICICI bank. They also suggested that improved customer satisfaction levels not only help in retaining existing customer but also attract new customers.[17]

Chandrika (2009) compared the performance of IT in banks, especially in PSBs. Overviewed, today’s banking technologies elaborates the computerization scenario in Indian banks, the advantage of private and foreign banks in using technology is more as compared to PSBs. Suggested that the PSBs to use IT both intensively and extensively for their in-house as well as external operations.[18]

Sharm and Thakur (2010) analyzed that customers of private sector banks are more satisfied about the ATM banking facility and I-banking facility as compared to the customers
of public sector banks. They also indicated that Interactive Voice Responsive System (IVRS) facility is not very commonly used by both public and private sector bank customer.[19] Chellani K. D. (2012) concluded that, to achieve E-banking policy goals under financial inclusion by end March 2012, RBI is framing appropriate policy of issuing licenses to corporate and other NBFCs to establish new banks with focus on to serve rural sector of the economy. [20]

2.1.3 Review from Reference Books:

Mathur (1978) in his book “Public Sector Banks in India's Economy - A Case Study of State Bank of India”; has evaluated the role of the public sector banks as an instrument for the rapid growth of the Indian economy. In the process of analyzing that role he has made a thorough study of the working of the State Bank of India and its seven subsidiaries[21]

Agarwall (1979) in his book “Management of Nationalized Commercial Banks in India with Reference to their Social Obligations” has assessed the performance of nationalized banks in discharging the various social obligations. There being no absolute line of measurement in this regard, an effort has been made to evaluate the performance of the nationalized banks in discharging the various social obligations on the basis of a comparison with the performance of other bank groups. For the assessment of their individual performance, the line of assessment adopted was the average performance of all the nationalized banks [22]

Seshadri (1981) in his book “Banks Since Nationalization” has analyzed the achievements of the nationalized banks with those that were left in the private sector. The progress achieved by these banks in the sphere of branches, deposits, advances etc. were analyzed with secondary data available from various banks, the Reserve Bank of India and so on. The efficiency and profitability of the nationalized banks too were analyzed. [23]

Agarwall (1982) in his book “Commercial Banking in India After Nationalization- A Study of their Policies and Progress” has analyzed the performance of commercial banks in India after nationalization. It was neither an empirical study nor the study of a particular aspect of commercial banking. It was only a study of banking development in the light of nationalization. Annual reports of banks, periodical reports of the Reserve Bank of India, personal discussion with bank officials and so on were the major sources relied on for the study.[24]

Hussain (1986) in his book “A Study of New Roles of the Public Sector Commercial Banking in India” has analyzed the major problems faced by the public sector banks in India. As national public sector institutions, they are required to face new challenges. How the new
developmental, organizational, managerial and functional problems can be solved. How best they can serve the priority sectors for economic regeneration and what should be the strategy for dynamic commercial banking policy in India - were some of the basic problems discussed in the book.[25]

Chawla (1987) in his book “Nationalization and Growth of Indian Banking” has investigated the development and growth of banking activities in India with particular reference to the state of Punjab. The analysis was carried out with the help of different types of growth rates; indices of changes were also calculated. Certain statistical tools like co-efficient of variation and rank correlation too were used in the study.[26]

Vishwanathan Bharathan (2008) has undertaken a study “Internet Banking- Some of the Contemporary Issues”. According to him, technology has made a tremendous impact in banking. ‘Anywhere, Anytime banking’ have become a reality. Also, it has thrown new challenges in the banking sector and new issues started cropping up which is going to pose certain problems in the near future. Author attempted to address the security and authentication issues in an internet banking and reiterates the point that online banking becomes less secure if users are careless, gullible or computer illiterate. With the globalization of business and services, our country cannot lag behind in niche area of internet banking. .[27]

Prabhu (1991) in his book “Excellence Through People: The Canara Bank Way”, explained how an organization can achieve its changing goals from time to time by following the right type of policies. He made an attempt to share his experiences, thoughts and views on creating and sustaining organizational excellence through people.[28]

Jagwant (1993) in his book “Indian Banking Industry: Growth and Trends in Productivity” examined the trends in productivity in public sector banks excluding the six banks nationalized in 1980. He analyzed the trends and changes in productivity, with particular emphasis on labor productivity and branch productivity. The trends, changes and differentials in productivity in different banks and bank groups were examined in detail based on seventeen indicators. The main source of data for the study was ‘Financial Analysis of Banks’ published by Indian Banks Association and Annual reports of banks.[29]

Rajendran (1993) in his book ‘Comparative study of the public sector and private sector banks during the year 1990-91’ chose three profitability ratios and six balance sheet ratios. He brought eight scheduled private sector banks, three nationalized banks and the State Bank of India within the purview of his study.[30]
Nitsure Rupa Rege (2006) in her book “E-Banking: Challenges and Opportunities”, she explained E-Banking has the potential to transfer the banking business as it significantly lowers the transaction and delivery costs. This book discussed about the problems faced by developing countries, (which have a low penetration of information and telecommunication technology), in realizing the advantages of E-banking initiatives for examples: the different operational environments for public and private sector banks, problems of security, authentication, management and regulation; also inadequate financing of small and medium scale enterprises (SME) were highlighted.[31]

2.1.4 Review from Committees:
The Committee on the Functioning of Public Sector Banks (1978) appointed by the Reserve Bank of India in 1977 made a broad evaluation of the performance of public sector banks in the country covering the spheres of branch expansion, deposit mobilization, credit disbursement, priority sector lending, efficiency, management - employee relations and so on. It made recommendations to ensure improvement in the efficiency of their operations and to restore their financial health. It made a pragmatic evaluation of the actual performance and functioning of the public sector banks during the period 1969 to 1977. It collected data from banks, bank staff, other financial institutions, commercial associations and so on.[32]

Working Group to consider feasibility of introducing MICR/OCR Technology for Cheque Processing (1982)
Recommendations: Introduction of 'item processing' (sorting and listing of cheques with the help of computers) in three phases. This process to be initiated:

• First phase: Four metropolitan cities viz. Mumbai, New Delhi, Chennai and Calcutta, with the help of MICR technology.
• Second phase: All state capitals and important commercial centers.
• Third phase: National clearing to be introduced by dividing the country into four regional grids with headquarters at Mumbai, New Delhi, Chennai and Calcutta. Each regional centre was to perform two functions: (i) to act as a clearing house for intra-grid instruments, and (ii) participate in national clearing on behalf of the grid for extra-grid outstation cheques.[33]

Committee on Mechanisation in the Banking Industry (1984)
• Chairman: Dr.C. Rangarajan, Deputy Governor, Reserve Bank of India.
Recommendations: 1) Banks should set up service branches at centers where they have more than 10 branches. The service branch so set up would exclusively be devoted to clearing operations of the bank at that particular centre. 2) Banks to be in readiness for the introduction of MICR clearing at the four metropolitan cities by assessing their requirements for encoders, adopting standardised cheque forms and reorganising work procedures where necessary, and training staff down to the branch level.[34]

Committees on Communication Network for Banks and SWIFT implementation (1987)
Chairman: Shri T.N.A. Iyer, Executive Director, Reserve Bank of India.
Recommendations: Committees recommends I) Setting up of X.25 based packet switching network called 'BANKNET' to be jointly owned by the Reserve Bank and the public sector banks. It suggested that the computer system resources of the four IBM Mainframes (installed at the four metros for cheque processing operations) could be made use of during the day time by BANKNET for data communication with additional equipment. 2) BANKNET to be implemented in two phases. In phase-I the computer systems available in the Head Offices of the public sector banks in the four metropolitan cities that would be connected to the four IBM Mainframe servers. In the phase-II connectivity could be gradually extended to eight to ten banking intensive centers and to a hundred centers over a three year period. The applications that were identified are: 1) inter-bank fund transfers on banks' own account and on customers' account 2) inter-branch funds transfers on banks' own account and on customers' account 3) currency chest transactions 4) government transactions 5) improvements in payment systems by facilitating automated clearing services 6) any branch banking, etc.
II) India should join the SWIFT (Society for Worldwide Interbank Financial Telecommunication) network for the transmission and reception of international financial messages.
III) BANKNET should strive to emulate SWIFT in matters of data security, encryption, and authentication and SWIFT message standards which are internationally accepted should be adopted by BANKNET.[35]

Committee on Computerisation in Banks (1988)
Chairman: Dr. C. Rangarajan, Deputy Governor, Reserve Bank of India
Major recommendations are: 1) Computerisation of the settlement operations in the clearing houses managed by Reserve Bank of India at Bhubaneshwar, Guwahati, Jaipur, Patna and
Thiruvananthapuram. 2) Operationalisation of MICR technology and the National Clearing of inter-city cheques at the four metropolitan cities. 3) Introduction of one-way collection of cheques drawn on the 4 metros received from Ahmedabad, Bangalore, Nagpur and Hyderabad. 4) Framing of uniform rules and regulations and of clearing houses. 5) Branch level computerisation and the establishment of connectivity between branches. 6) Improvements in customer service - introduction of on-line banking. 7) Standardisation and rigorous security features to ensure an efficient and risk free transfer of funds electronically. 8) Setting up a network of automated teller machines (ATMs) in Mumbai. ATMs to be strategically located at airports, railway stations, hospitals, important commercial centers, as well as bank branches, to be used by the customers to perform a variety of functions such as deposits, withdrawals, balance enquiries, statement of accounts etc., at any point of time during the day. 9) Introduction of a single 'All Bank' credit card and advocated the need for its widespread acceptance by merchant establishments and usage by customers to reduce the load on cash and cheque transactions.[36]

**Dr. Rangrajan Committee Report (1989)** A 16-member committee with Dr. C.Rangarajan (the then Deputy Governor of RBI) was formed in 1988 to make recommendations for computerization in banking industry in nationalized banks. The major recommendation of this committee are: 1) Regional office/ Zonal office/ Head office should be computerized 2) All branches located in top 30 centers (which constitute about 51% of total business) should be computerized 3) Branches having average 750 vouchers per day (during preceding 52 weeks) should be computerized 4) BANKNET and SWIFT to be used by banks 5) On-line terminals should be given at the premises of corporate customers.[37]

**Goiporia Committee (1991)** Reserve Bank of India appointed this committee on customer service in Banks (1991). It undertook a detailed customer survey covering different categories of bank customers. The Committee made 97 wide ranging recommendations to improve the customer service in banks.[38]

**The Committee on the Financial System (1992)** appointed by the Government of India (Narasimhan Committee), in 1991 examined all aspects relating to the structure, organization and functions of the Indian financial system. It made wide ranging recommendations with a view to ensuring flexibility, functional autonomy and thereby enhancing efficiency, productivity and profitability of the banking sector and the financial system. It examined the cost, composition and adequacy of the capital structure of the various financial institutions and reviewed the relative roles of the different types of financial institutions in the financial system. It recommended ways to improve the efficiency and effectiveness of the system with
the emerging credit needs of the economy. Its recommendations include, inter alia capital adequacy norms, prudential norms for income recognition, provisioning for bad debts, transparency of bank balance sheets, liberal branch licensing policy and so on. [39]

Committee on Technology Issues relating to Payments System, Cheque clearing and Securities Settlement in the Banking Industry (1994)
Chairman : Shri W.S. Saraf, Executive Director, Reserve Bank of India

Recommendations: 1) Establishment of an Electronic Funds Transfer (EFT) system, with the BANKNET communications network as its carrier. The message transfers would be in a batch mode with high value institutional funds transfers being batched every one hour and the transactions of retail customers being batched at the end of the day. Starting with the 4 metropolitan cities, the scheme to be extended in a phased manner to all important centers. 2) Enactment of suitable legislation on the lines of the electronic funds transfer Act 1978, USA and Data Protection Act 1984, UK. 3) Magnetic ink character reader (MICR) clearing is introduced at all centers with more than 100 bank branches. Priority should be given to centers such as Ahmadabad, Bangalore, Hyderabad, Pune and Surat which have relatively large volumes. 4) Introduction of a Delivery versus Payment (DvP) system for SGL transactions, with settlement on gross basis both for securities transactions in PDO and funds transactions in current accounts at DAD. 5) Introduction of electronic clearing service credit for low value repetitive transactions such as interest, dividend, salary, pension payments and an electronic debit clearing for payments to utility companies. 6) A uniform size for MICR instruments. 7) Switch over to on-line inter-bank clearing on a gross basis. 8) Introduction of 'Clearing Bank' concept for decentralised cheque processing. 9) Truncation of cheques up to the value of Rs.5,000/- 10) Large scale induction of computers and communication technology in service branches 11) Optimal usage of SWIFT. 12) NICNET to be used for the reporting of currency chest transactions by the chest branches to their link offices and issue departments of the RBI. 13) Promotion of a card culture, as well as enhanced training facilities. [40]

Committee for proposing legislation on Electronic Funds Transfer and other Electronic Payments (1995)
Chairperson: Smt. K.S. Shere, Principal Legal Adviser, Reserve Bank of India.

Recommendations: 1) EFT system could be introduced immediately by framing regulations under Section 58 of the RBI Act. A model customer contract agreement to govern the banker-customer relationship with regard to EFT should be adopted by all banks participating
in the system. 2) As a long term measure, a new legislation needed for regulating, defining and determining the rights and obligations of the system providers and users.[41]

The PEP Committee on Banking (1997) they constituted to study the productivity, efficiency and profitability of commercial banks used four criteria; namely- productivity, social objectives-spatial, social objectives-sectoral and profitability. Under each criterion, it used a set of indicators. It also examined aspects like planning, budgeting, marketing, management information systems, annual accounts, audit systems, procedures and so on. It analyzed banking costs, profitability of operations, pricing of bank services, trends in earnings and expenditures etc. and made a number of recommendations. The study was experimental in nature and it categorically stated that the set of indicators used by it does not represent either the first or the last choice.[42]

Major Recommendations of Vasudevan Committee on Technology Upgradation in Banking Sector (1999)

Communication infrastructure and usage of INFINET: Improving effectiveness if VSAT network aims to enhance the transponder capacity to the extent feasible and the number of out routes as the demand grows. For inter-bank and intra-bank applications, it is necessary to have an application architecture keeping in mind that the INFINET backbone network will be VSAT based.

Standardization and Security:

- RBI may consider appointing IDRBT as the certification agency for security management.
- Banks should adopt widely used standard of cryptography procedures to prevent data tamper during transmission.
- Technology should be allowed to evolve into standard-based solutions for multi-vendor heterogeneous environment working co-operatively and collectively for EFTPoS, including the debit, credit and smart cards based operations.
- Computerization of Government Transaction
- There is a need to computerize all branches of banks dealing with government transactions.
- The computerization of government departments should be synchronized with the computerization of bank branches dealing with government transaction.
All PAOs/Circle offices should be computerized not later than March 31, 2001 and DDO/Treasury offices before March 31, 2002 in alignment with the computerization of FPBs and dealing branches.

Legal Framework for Electronic Banking:
The Reserve Bank may promote amendment to the Reserve Bank of India Act, 1934 and assume the regulatory and supervisory powers on payment and settlement systems. Simultaneously, the RBI may promote a new legislation on Electronic Funds Transfer System to facilitate multiple payment system, to be set up for facilitate multiple payment system, to be set up for banks and financial institutions. The RBI and IBA should pursue with the Department of Telecommunications (DoT)/other competent Authority to permit encryption of data files/messages transmitted through communication channels for facilitating easier access to remotely located branches to the INFINET network.[43]

Report of the working group on electronic money (2002),
Chairman Mr. Zarir J. Cama
In order to preserve effectiveness of monetary policy and integrity of e-money schemes, the Group suggests following six recommendations- (i) Prudential supervision: Issuers of electronic money must be subject to prudential supervision. (ii) Solid and transparent legal arrangements: The rights and obligations on the part of the respective participants (customers, merchants, issuers and operators) in an electronic money scheme must be clearly defined and disclosed. Such rights and obligations must be enforceable under all relevant jurisdictions. (iii) Technical security: Electronic money schemes must maintain adequate technical, organisational and procedural safeguards to prevent, contain and detect threats to the security of the scheme, particularly the threat of counterfeits. (iv) Protection against criminal abuse: Protection against criminal abuse, such as money laundering, must be taken into account when designing and implementing electronic money schemes. (v) Monetary statistics reporting: Electronic money schemes must supply the central bank with whatever information that may be required for the purposes of monetary policy. (vi) Redeemability: Issuers of electronic money must be legally obliged to redeem electronic money against central bank money at par at the request of the holder of electronic money vii) Reserve requirements: The possibility must exist for central banks to impose reserve requirements on all issuers of electronic money.[44]

The Group addresses IT issues across multiple dimensions like IT Governance, Information security, IT operations, Information system audit, cyber fraud, business continuity planning, customer education and legal issues arising out of the use of IT and provide recommendations in these areas. The working group was divided into five sub-groups with the undernoted specific focus areas:

- Technology issues – Information security
- IT Governance and IS Audit
- Operational issues – IT operations, cyber fraud
- Legal issues
- Customer education

The objective before groups was to provide a set of guidelines to banks covering the entire gamut of electronic banking. This would in part serve as a common minimum standard for all banks to adopt and in other part lay down the best practices which are recommended for adoption by banks in a phased manner. Which provides safer and sounder banking environment. It was felt that there was a need for banks to follow a consistent approach in each focus area, to minimize differing interpretations. [45]

**Working Group report on Cloud computing option for Urban Cooperative Banks (2012), Shri A. K Hirve - Member Secretary**

The working group reviewed its terms of references in the context of the emerging trends and experiences. Following recommendations are made in this context:

- As cloud computing is an emerging technology for which standards and technology management processes are still evolving. It has many complexities and uncertainties which need to be understood. In view of the sensitive nature of banking services as well as limitations of the target banks for managing this technology, the working group recommends caution while adopting cloud computing solutions for the banks.

- In respect of banks where such innovative cloud like solutions are already deployed on a private cloud, the working group recommends that the issues identified in this report may be examined. Also need adequacy of risk mitigation measures and to address concern regarding data security and data privacy in the multi-tenancy environment.

- Cloud computing be a developmental activity which can be taken up separately and the experience in this regard could be shared to understand the workings of the cloud solutions.
As revealed from the experience outside India as well as the suggestions received from the major industry players, the working group perceives a need for further research and development particularly in the area of cloud governance, cloud management and security technology for cloud computing. Initiative in this regard probably needs to be from the banking and software industry whereas the regulatory authorities could make use of such research input at a later date.[46]

2.1.5 Review from Conferences:

Varde (1998) he distinguished between effectiveness, efficiency and productivity. He classified the efficiency of a bank into four categories, i.e., (1) manpower efficiency (2) operational efficiency (3) commercial efficiency and (4) efficiency of ancillary business. Efficiency under each category can be measured separately, and measure of efficiency can be considered as productivity. [47]

Bankers Training College (1998) he made an attempt to bring out the factors generally affecting efficiency and productivity. It recognized that business per employee and ratio of average business to establishment expenses are the most popular indicators of productivity. However it favored a 'Disaggregated Approach' for measuring the efficiency and productivity of banks. Department of Banking Operations and Development.[48]

Sooraj and Ganti (1993) in their paper “Comparative performance of Public Sector Banks in India” used the taxonomic method to measure inter-bank comparisons of performance of twenty eight public sector banks in India. In their study the bank performance index is based on three income indicators - percentage of interest and discount income , commission and brokerage - income and other income – and three expenditure indicators - percentage of interest expenses , manpower expenses and other expenses. The analysis was carried out with the help of differential weights and equal weights to each variable[49]

Padhy and Swar (2009) objective is to investigate the role of technology in banking and its impact on perceived SQ in public, private and foreign banks in Orissa. 300 customers (150 from public, 125 from private and 25 from foreign banks) through a structured questionnaire. SERVQUAL and Crosby’s total quality training programme were tested. Gap scores (mean difference between expectations and perceptions) technique is used. Observed that, foreign
bank was found to very close to the expectations of customers followed by ICICI and AXIS bank in private sector whereas the SQ of public sector banks was found to be very low as SBI was ranked lowest on tangibility and responsiveness and PNB was ranked lowest on assurance and empathy.[50]

2.1.6 Review from Ph. D. Thesis:

Saraswat S.B. (1995) studied bank services of United Western Bank Ltd., and The Sangli Bank Ltd. in his thesis marketing environment for a product consist of i) the organization ii) the markets iii) the economy iv) the technology v) the law and politics vi) the customer and social environment. Among this the technologically, Indian banking is still struggling to find a way to total modernization. Technology upgradation shall help the Indian banks to reach new heights in business developments. However, they had to remove the fear and apprehension from the minds of their workman and clients.[51]

Yallatti R.M. (2003) analyzed implementation of 7 P’s of marketing in bank services. Study is conducted in Sangli district, with 2 co-operative banks, one private and one national banks. 200 customers opinion about bank facilities such as i) Deposit account facility ii) Cash credit facility iii) Overdraft facility iv) Labor facility v) Loan facility vi) Bank employees vii) Bank management and vii) The banks. Hypotheses tested using coefficient of variation (CV) and the study shows that customers are more satisfied with co-operative bank facilities than national and private bank facility irrespective of overdraft credit and loan facility.[52]

Kumbhar V.M. (2011) attempts to identify the alternative banking and its customer satisfaction. A study is done on four national and two private sector banks in satara city with 190 customers. “eBankQual instrument” is designed to access service quality and customer satisfaction in alternative banking services. Results of the study shows that, education and profession has positively affecting the customers satisfaction. However, income levels of the respondents are not significant demographic factor in customer satisfaction. Also he conclude that there is significant difference in service quality and customer satisfaction level of customers in public and private sector banks.[53]

2.1.6 Conclusion:

It is conclude that most of the researcher has studied the service quality (SQ) factor in Private, Public and foreign banks on the basis of service provided by them using SERVQUAL method. Also some research work is done on measuring customer satisfaction in private, public and foreign banks. Committees established by RBI to implement new
technology in banking sector for cost reduction in service and for providing convenient and secure services to customers.

Present study is extension of above work, which measures service user’s satisfaction on the basis of service quality and transparency maintained in E-banking services by the public and private sector banks. For the study purpose the E-banking services like ATM, Internet, Mobile, RTGS, EFT/NEFT, Fund transfer which are used by the service users in Sangli district has been considered.

References-


38. Reserve Bank of India Committee on Customer Service in Banks (1991)


42. Report of the Productivity, Efficient and Profitability (PEP) Committee on Banking, (Headed by .C. Luther), Reserve Bank of India. 1977.


II CONCEPTUAL FRAMEWORK OF E-BANKING:

2.2.1 Introduction:

Since its inception, E-banking has experienced strong and sustained growth. World bank report on growing economy in e-finance pointed out that the three countries with impressive progress in information technology. These three countries are Estonia, Republic of Korea and Brazil (Claessens et al 2001). where creation of the world’s leading electronic banking systems has been done at a remarkably low cost compared to other world-class internet banks (Sahlen 2002).

Both in the United States and in Europe, internet banking operations currently represent between 5 per cent and 10 per cent of the total volume of retail banking transactions. According to Jupiter Media, Internet traffic for all United States banks grew by 77.6 per cent between July 2000 and July 2001, compared with overall World Wide Web traffic growth of 19.8 per cent over the same period. Another source estimated that the share of United States households using Internet banking will increase from 20 per cent in 2001 to 33 per cent in 2005, and from by 2010 there are more than 55 billion users. Jeevan (2000) notes that with rigid controls is giving way to deregulation, banks are gearing up their communications infrastructure to obtain a competitive edge from E-banking. Thus it is fast becoming a reality in India. A. Nair (1999), pointed out that E-banking is fast becoming a strategic necessity for most commercial banks, as competition increases from private banks and NBFIs. Though de-regulation may have had an impact on the banking industry in general. The Indian infrastructure itself is in problematic state, by a lack of PC penetration (there is an estimated 2 million units for a population close to 1 billion according to Gupta and Storey, 1999) and low telephone penetration (19.1 million in 1999).

Due to this, India has got low E-banking adoption rates, low labor costs and “free” existing branches. There is a better price discovery process as more and more markets gain integrated real-time and improved access to these trading and data-dissemination platforms. At the same time, however, many changes are still required in technology, access infrastructure and banking regulation. Virtually all banks use banking software at their head offices and during the past few years around one third of local banks has become society for worldwide inter-bank financial telecommunication (SWIFT) members. A quarter of local banks, provide Credit card and point of sale services (POS); while in major cities, ATM and internet banking are expanding rapidly. (Raihan, 2001).
2.2.2 Core Banking Solution (CBS):

In bringing synergy between different banks, core banking solution will set as a facilitator. CBS is a model in which all branches of a bank are connected to the central bank. Most banks are actively looking at centralized core banking solutions as a tool for their future business growth. Multiple channels of banking are getting integrated. Banks are now looking to provide a “one-view” solution to customers across all service lines. ATMs are getting shared through ATM networks and Security of the technology infrastructure is assured by disaster recovery centers that are being set up. Every ATM center has become so customer-friendly that the customer now prefers to transact his business through machines. An entirely new shape has been given by Internet banking to the business of banking.

A single channel provides multiple services like ATM, debit card, internet banking, mobile banking etc. The process ensures connectivity of identified branches, regional offices, zonal offices and central office departments.

CBS will ensure the establishment of a reliable centralized data repository for the bank. The implementation of integrated customer-centric services like online ATMs, cash management services will be ensured by CBS.\[8\]

2.2.3 Automated Teller Machine (ATM):

An Automated Teller Machine (ATM), is also known as Automated Banking Machine (ABM) or Cash Machine. ATM supports for financial transactions of users from financial institution in a public space without the need for a bank cashier, clerk or any bank employee.

ATM consist of plastic ATM card having magnetic strip which contains detail users information, card number, some security information. Authentication is provided by the entering of customer’s personal identification number (PIN).

Customers can access their bank accounts by using an ATM, in order to make cash withdrawals, credit card cash advances, to check their account balances as well as purchase prepaid cell phone credit. If the currency being withdrawal from the ATM is different from that, which the bank account is denominated in the money will be converted at a wholesale exchange rate. Thus, ATMs often provide the best possible exchange rate for foreign travelers \[10\] and are heavily used for this purpose as well.

2.2.3.1 History:
In Japan, Sweden, the United States (US) and the United Kingdom (UK) initially the idea of self-service in retail banking is developed through independent and simultaneous efforts. In the USA, Luther George Simjian has been credited with developing and building the first cash dispenser machine. There is a strong evidence to suggest that Simjian worked on this device before 1959 while his 132nd patent (US3079603) was first filed on 30 June 1960 (and granted 26 February 1963). The rollout of this machine, called Bankograph, was delayed a couple of years. This was due in part to Simjian's Reflectone Electronics Inc. being acquired by Universal Match Corporation. An experimental Bankograph was installed in New York City in 1961 by the City Bank of New York, but removed after 6 months due to the lack of customer acceptance. The Bankograph was an automated envelope deposit machine (accepting coins, cash and cheques) and it did not have cash dispensing features. While the concern of European and Asian banks was cash distribution, the Bankograph, however, embodied the preoccupation by US banks in finding alternative means to capture core deposits.

In Tokyo in 1966, a first cash dispensing device was used. Although little is known of this first device, it seems to have been activated with a credit card rather than accessing current account balances. This technology didn’t have immediate consequence in the international market.

During the early 1960’s, in simultaneous and independent efforts, engineers in Sweden and Britain developed their own cash machines. The first of these that was put into use, was by Barclays Bank in Enfield Town in North London, United Kingdom on 27 June 1967. This machine was the first in the UK and was used by English comedy actor Reg Varney, at the time so as to ensure maximum publicity for the machines that were to become mainstream in the UK. This instance of the invention has been credited to John Shepherd-Barron, while disregarding other engineers at De La Rue instruments. Nevertheless, Shepherd-Barron was awarded an OBE, in the 2005 New Year’s Honors list. As plastic bank cards had not yet been invented, his design was used in special checks that were matched with a personal identification number (PIN).

The idea of a PIN stored on the card was developed by a British engineer working in the MD2 named James Good fellow in 1965. The essence of this system was that is it enabled the verification of the customer with the debited account without human intervention. This patent is also the earliest instance of a complete “currency dispenser system” in the patent record. This patent was filled on 5 March 1968, in the USA and granted on 1 December 1970. It had a profound influence on the industry as a whole. Not only did future entrants into the
cash dispenser market such as NCR Corporation and IBM licence Goodfellow’s PIN system, but a number of later patents references this patent as “Prior Art Device” [19]

2.2.3.2 ATM Service in India:

HSBC - the Hongkong and Shanghai Banking Corporation - was the first bank to introduce the ATM concept in India way back in 1987. In India, the introduction of HSBC Bank can be dated as early as the year 1853, with the establishment of the Mercantile Bank of India in Mumbai [20]

2.2.3.3 ATMs Alternative uses:

ATMs were originally developed as just cash dispensers. ATMs have been evolved to include many other bank-related functions. In some countries, especially those which benefit from a fully integrated cross-bank ATM network (e.g.: Multibanco in Portugal), ATMs include many functions which are not directly related to the management of one's own bank account, such as:

- Deposit currency recognition, acceptance, and recycling.
- Paying routine bills, fees, and taxes (utilities, phone bills, social security, legal fees, taxes, etc.).
- Printing bank statements.
- Updating passbooks.
- Loading monetary value into stored value cards.
- Purchasing products.
- Postage stamps.
- Lottery tickets
- Train tickets
- Movie tickets
- Shopping mall gift certificates
- Games and promotional features
- Donating to charities
- Cheque Processing Module
- Adding pre-paid cell phones / mobile phone credit.
- Paying (in full or partially) the credit balance on a card linked to a specific current account.
Banks are trying to use the ATM as a sales device to deliver pre-approved loans and targeted advertising using products such as ITM (the Intelligent Teller Machine) from CR2 or Aptra Relate from NCR. ATMs can also act as an advertising channel for companies to advertise, their own products or third-party products and services. [21]

2.2.3.4 Future Developments in ATMs:

On ATMs, several different technologies have been demonstrated and deployed by manufacturers; that have not yet reached worldwide acceptance, such as: biometrics, where authorization of transactions is based on the scanning of a customer's fingerprint, iris, face, etc. Biometrics on ATMs can be found in Asia. While manufacturing ATMs, following upgradation points should be taken into consideration, in future:

- Bar code scanning.
- On-demand printing of "items of value" (such as movie tickets, traveler's cheques, etc).
- Dispensing additional media (such as phone cards).
- Co-ordination of ATMs with mobile phones.
- Customer-specific advertising.
- Integration with non-banking equipment. [22]

2.2.4 Magnetic Ink Character Recognition (MICR)

A character recognition technology i.e. ‘Magnetic Ink Character Recognition’, or MICR, is used primarily by the banking industry to facilitate the processing of cheque. The technology allows computers to read information (such as account numbers) of printed documents. MICR codes can be easily read compared to barcode, by humans.

By using a magnetic ink or toner, usually containing iron oxide, MICR characters are printed in special typefaces. As a machine decodes the MICR text, it first magnetizes the characters in the plane of the paper. Then the characters are passed over a MICR read head, a device similar to the playback head of a tape recorder. As each character, passes over the head it produces a unique waveform that can be easily identified by the system.

The use of magnetic printing allows the characters to be read reliably even if they have been overprinted or obscured by other marks, such as cancellation stamps. The error rate for the magnetic scanning of a typical check is smaller than with optical character recognition systems. For well printed MICR documents, the "can't read" rate is usually less than 1%
while the substitution rate (misread rate) is in the order of 1 per 100,000 characters. ISO 1004:1995 standardizes MICR. [23]

2.2.4.1 Fonts used in MICR:

The popular MICR fonts E-13B and CMC-7, are used around the world. In the 1960s, the MICR fonts became a symbol of modernity or futurism, leading to the creation of lookalike "computer" typeface that imitated the appearance of the MICR fonts, which unlike real MICR fonts, had a full character selection.

There are 14 characters in E-13B font. The control characters bracketing each numeral block are (from left to right) transit, on-us, amount, and dash. Almost all Indian, US, Canadian and UK cheques use the E-13B font. (The "13" in the font's name refers to the 0.013 inch grid used to design it.). Decimal digits contains the following symbols:

1. ⑆ called as transit, it is used to define a bank branch routing transit number.

2. ⑇ called as amount, it is used to denote a transaction amount.

3. ⑧ called as on-us, it is used to define a customer account number.

4. 〃 called as dash, it defines parts of numbers, e.g., routing numbers or account numbers.

In the late eighties this technology was first used in India at the four major metropolitan cities of Mumbai, Chennai, New Delhi and Kolkata. These centers were set up and are managed by the Reserve Bank of India. The success of these MICR based local clearing processing centers. The initiatives on the part of commercial banks for setting up of many more MICR based cheque processing centers at commercially important centers of the country with the latest technology. Some centers have also got the facility for ‘imaging’ which enables capturing of the digital images of the cheques.

There is a requirement of standard format and defined size of 8” x 3 2/3”, to facilitate MICR based cheque processing, instruments passing through clearing. The instruments should be printed on MICR grade quality paper with a "read band" of 5/8" in width reserved at the bottom on which essential particulars occur in special MICR ink in the E-13B font[24].

2.2.4.2 MICR in India:

In 1987, MICR was introduced in the four Metros in India. The MICR clearing is now in operation in 14 centers (Hyderabad, Banglore, Ahmedabad, Kanpur, Jaipur, Nagpur,
Baroda, Pune, Guhati, Trivandrum). It was proposed to be extended to a total of 22 centers where volume of clearing transactions was large.

2.2.5 Real Time Gross Settlement (RTGS):

RTGS is an electronic payment system. This "electronic" payment system is normally maintained or controlled by the central bank of a country. There is no physical exchange of money; the central bank makes adjustments in the electronic accounts of bank A and bank B, reducing the amount in bank A's account and increasing the amount of bank B's account by the same. Real Time Gross Settlement (RTGS) is funds transfer systems where transfer of money or securities takes place from one bank to another on a "real time" and on "gross" basis. Settlement in "real time" means payment transaction is not subjected to any waiting period. The transactions are settled as soon as they are processed. "Gross settlement" means the transaction is settled on one to one basis without bunching or netting with any other transaction. Once processed, payments are final and irrevocable.

RTGS payments are irrevocable once processed. The RTGS system is suited for low-volume, high-value transactions. It lowers settlement risk, besides giving an accurate picture of an institution's account at any point of time. Such systems are an alternative to systems of settling transactions at the end of the day, also known as the Net Settlement. In this system, all the inter-institution transactions during the day are accumulated. At the end of the day, the accounts of the institutions are adjusted. The implementation of RTGS systems by Central Banks throughout the world is driven by the goal to minimize risk in high-value electronic payment settlement systems.

Any RTGS employs two sets of queues: one for testing outgoing funds availability on a chronological FIFO basis with the option of prioritizing specific inquiries, while the other queue is for processing debit/credit requests received from the central bank's integrated accounting system. In an RTGS system, transactions are settled across accounts held at a central bank on a continuous gross basis. Settlement is immediate, final and irrevocable. Credit risks due to settlement lags are eliminated. RTGS does not require core banking to be implemented across participating banks, since transactions are direct, with no central processing or clearing operations. [25]

2.2.5.1 Working of RTGS

The financial intermediaries can settle interbank transfers for their own account as well as for their customers as RTGS is a large value (minimum value of transaction should be
₹ 2,00,000) funds transfer system. The system effects final settlement of interbank funds transfers on a continuous, transaction-by-transaction basis throughout the processing day. Customers can access the RTGS facility between 9 am to 4:30 pm on week days and 9 am to 12 noon on Saturday.[26]

For RTGS transactions, banks should have 11 character alphanumeric codes, which are required for transactions along with recipients account number. Fees for RTGS vary from bank to bank. Both the remitting and receiving must have core banking in place to enter into RTGS transactions.

2.2.5.2 RTGS in India

RTGS is managed by RBI. In India RTGS System was implemented since March 26, 2004.

2.2.6 Electronic Funds Transfer (EFT):

The electronic exchange or transfer of money from one account to another i.e., either within a single financial institution or across multiple institutions, through computer-based system is known as Electronic funds transfer (EFT)s. The term is used for a number of different concepts:

- Cardholder - initiated transactions, where a cardholder makes use of a payment card.
- Direct deposit payroll payments for a business to its employees, possibly via a payroll service bureau.
- Direct debit payments, sometimes called electronic checks, for which a business debits the consumer's bank accounts for payment for goods or services.
- Electronic bill payment is online banking, which may be delivered by EFT or paper cheque.
- Transactions involving stored value of electronic money, possibly in a private currency.
- Wire transfer via an international banking network (generally carries a higher fee).

2.2.6.1 EFT in India

To help banks offering their customers, EFT is a scheme introduced by RBI. The money transfer service is provided from account to account of any bank branch to any other bank branch in places; where EFT services are offered.

- Banks with EFT System

All the branches of the 27 public sector banks and 55 scheduled commercial banks at the 15 centres (viz., Ahmedabad, Bangalore, Bhubneshwar, Kolkata, Chandigarh, Chennai,
Guwahati, Hyderabad, Jaipur, Kanpur, Mumbai, Nagpur, New Delhi, Patna and Thiruvananthapuram) are covered by the EFT system. Funds transfer is possible from any branch of these banks at these centers to other branch of any bank at these centers both inter-city and intra-city. If the remitting bank transmits the funds, transfer message to RBI so as to hit the first settlement at 12 noon, the receiving bank’s account is credited by RBI at the destination centre and beneficiary gets the credit on Day 1 itself. If the same is included in subsequent settlements i.e., between 2 p.m. and 4 p.m., the beneficiary gets credit on Day 2.

2.2.6.2 Working of EFT:

Step-1: The remitter fills in the EFT application form giving the particulars of the beneficiary (city, bank, branch, beneficiary’s name, account type and account number) and authorizes the branch to remit a specified amount to the beneficiary by raising a debit to the remitter’s account.

Step-2: The remitting branch prepares a schedule and sends the duplicate of the EFT application form to its Service branch for EFT data preparation. If the branch is equipped with a computer system, data preparation can be done at the branch level in the specified format.

Step-3: The Service branch prepares the EFT data file by using a software package supplied by RBI and transmits the same to the local RBI (National Clearing Cell) to be included for the settlement at 12 noon, 2 p.m. and 4 p.m.

Step-4: The RBI at the remitting centre consolidates the files received from all banks, sorts the transactions city-wise and prepares vouchers for debiting the remitting banks on Day-1 itself. City-wise files are transmitted to the RBI offices at the respective destination centers.

Step-5: RBI at the destination centre receives the files from the originating centers, consolidates them and sorts them bank-wise. Thereafter, bank-wise remittance data files are transmitted to banks on Day 1 itself. Bank-wise vouchers are prepared for crediting the receiving banks’ accounts the same day or next day.

Step-6: On day 1/2 in morning the receiving banks at the destination centers process the remittance files transmitted by RBI and forward credit reports to the destination branches for crediting the beneficiaries’ accounts. [30]

Electronic Funds Transfer EFT System hosted and operated by the RBI, permits transfer of funds, upto ₹ 5 lacs from any account at any branch of any member bank in any city to any other account at any branch of any member bank in any other city. This system utilizes the Service Branches of the member banks and the nodal offices of RBI. RBINET is the conduit for the flow of funds. The Reserve Bank of India acts as the service provider as well as
regulator. A special EFT (SEFT) was introduced in April 2003, covering about 3000 branches in 500 cities.

2.2.7 National Electronic Fund Transfer (NEFT):

History of NEFT

The NEFT system came into effect from 21 November 2005. NEFT was set to cover all banks which were participating in the special electronic funds transfer (SEFT) clearing. NEFT was made on the structured financial messaging solution (SFMS) platform and is public key infra structure (PKI) enabled. RBI made it mandatory to migrate all the SEFT banks to NEFT by 15 December 2005. As NEFT would be serving all the bank customers using SEFT, the SEFT system was discontinued from 1 January 2006. Banks which fulfilled the eligibility criteria for participation in RTGS were invited by RBI to participate in the NEFT. As on November 30, 2010 there are more than 72,000 RTGS enabled bank branches [27].

For transferring funds of Indian financial institution (especially banks), National electronic funds transfer (NEFT) is an online system. This facility is used mainly to transfer funds below ₹ 2, 00,000. The Reserve Bank of India has instructed banks that they should not use RTGS for amounts below ₹ 2 lacs. The new rule came into effect on November 15, 2010 for small transactions; RBI has given permission to banks for offering NEFT services.

2.2.7.1 RTGS and NEFT:

RTGS is on gross settlement basis, while NEFT is on net settlement basis this is the key difference between RTGS and NEFT. Besides, RTGS facilitates real-time transfer, while NEFT involves eleven settlements from 9 a.m. to 7 p.m. on week days and five settlements from 9 a.m. to 1 p.m. on Saturdays. Thus, if a customer has given instruction to its bank to transfer money through NEFT to another bank in the morning hours, money would be transferred the same day, but if the instruction is given later during the day, money would be transferred next day.

However, RTGS facility is available in over 72,000 branches, while NEFT is available in little over 70,000 branches of 106 banks (in December 2010). Besides, while all commercial banks have put in place the RTGS facility, only 43 banks have purchased the software required to facilitate NEFT based transaction. RBI has instructed banks that all branches which are RTGS enabled should also provide NEFT by December 2006. Sources said that RBI also had planned to discontinue EFT. This is because EFT is available only in 15 locations; where RBI has its clearing house.
The minimum transaction value for RTGS is ₹ 2,00,000; whereas there is no minimum value for NEFT.[28]

2.2.8 Automated Clearing House (ACH):

Automated Clearing House (ACH) payments are used by both government and commercial banks. Businesses are also increasingly by using ACH to collect and transfer cash from customer’s online, rather than accepting credit or debit cards. Thus ACH is an electronic network for financial transactions. ACH processes large volumes of credit and debit transactions in batches. ACH credit transfers include direct deposit payroll and vendor payments. ACH direct debit transfers include consumer payments on insurance premiums, mortgage loans and other kinds of bills.

For governing the ACH network, NACHA (National Automated Clearing House Association) and the Federal Reserve Bank establish rules and regulations. In 2002, this network processed an estimated 8.05 billion ACH transactions with a total value of $21.7 trillion. (credit card payments are handled by separate networks).

Collectively, the nation's largest automated clearing house operator is the Federal Reserve Bank and in 2005 it processed 60% of commercial interbank ACH transactions. The electronic payment network (EPN), the only private sector ACH operator in the U.S., processed the remaining 40%. Fed ACH is the Federal Reserve's centralized application software used to process ACH transactions. EPN and the Reserve Banks rely on each other for the processing of some transactions when either party to the transaction is not their customer. These interoperate transactions are settled by the Reserve Banks. In the early and mid 90s, a beginning was made in introducing ACH services such as electronic clearing service and electronic funds transfer.

An enhanced offering is being offered by the Federal Reserve Banks for cross-border electronic payments that will be enabled by the International ACH Transaction rule. In anticipation of the upcoming implementation of NACHA's international ACH transaction (IAT) rule, the Federal Reserve Banks are introducing ‘FedGlobal’ ACH services, an enhanced suite of services designed to offer an efficient means for cross-border electronic payments to more than 30 countries in Europe and Latin America. The Federal Reserve has provided outbound cross-border ACH payments to Canada, Mexico, and several European countries.

2.2.8.1 ACH in India:

Within the Rules and regulations governing the ACH network are established by the Reserve Bank of India with the help of the State Bank of India.
2.2.9 Electronic Clearing Services (ECS):

ECS is a mode of electronic funds transfer from one bank account to another bank account using the services of a Clearing House. This is normally for bulk transfers from one account to many accounts or vice-versa. This can be used both purposes. First one is, for making payments like distribution of dividend, interest, salary, pension, etc. Second one is, by institutions or for collection of amounts for purposes such as payments to utility companies like telephone, electricity, or charges such as house tax, water tax, etc. or for loan installments of financial institutions/banks or regular investments of persons.

2.2.9.1 Types of ECS-

There are two types of ECS called ECS (Credit) and ECS (Debit).

**ECS (Credit)** is used for affording credit to a large number of beneficiaries by raising a single debit to an account, such as dividend, interest or salary payment.

**ECS (Debit)** is used for raising debits to a number of accounts of consumers/ account holders for crediting a particular institution.

2.2.9.2 Working of ECS:

Any institution can initiate ECS payments (called ECS user) ;which has to make bulk or repetitive payments to a number of beneficiaries. They can initiate the transactions after registering themselves with an approved clearing house. ECS users have also to obtain the consent as also the account particulars of the beneficiary for participating the ECS clearings.

The sponsor bank i.e. the ECS user's bank, under the scheme and the ECS beneficiary account holder is called the destination account holder. The destination account holder's bank or the beneficiary's bank is called the destination bank. The beneficiaries of the regular or repetitive payments can also request the paying institution to make use of the ECS (Credit) mechanism for effecting payment. The ECS users intending to effect payments have to submit the data in a specified format to one of the approved clearing houses. The list of the approved clearing houses or the list of centers; where the ECS facility has been provided is available at www.rbi.org.in.

The account of the ECS user would be debited by the clearing house through the account of the sponsor bank on the appointed day and credit the accounts of the recipient banks, for affording onward credit to the accounts of the ultimate beneficiaries.

2.9.3 Advantages of ECS
Paper handling creates a lot of pressure on banks as they have to encode the instruments, present them in clearing, monitor their return and follow up with the concerned bank and customers. This problem can be eliminated by using ECS.

In ECS banks simply get the payment particulars relating to their customers. All they need to do is to match the account particulars like name, a/c number and credit proceeds. Wherever the details do not match, they have to return it back, as per the procedure. [29]

2.2.9.4 ECS in India:
ECS Scheme operated by the RBI since 1996-97. The clearing and settlement activities are dispersed through 1,047 clearing houses managed by RBI, the State Bank of India and its associates, public sector banks and other institutions.

2.2.10 Credit card and Debit Cards:
2.2.10.1 Credit Cards:

Credit card is one of the alternatives for electronic payments. A credit card is a small plastic card issued to users for payment purpose. It allows its holder to buy goods and services based on the holder's promise to pay for these goods and services. The issuer of the card creates a turning account and grants a line of credit to the user from which the user can borrow money for payment to a merchant. It also used for the cash advance to the user.

A continuing balance of debt, subject to interest being charged are allowed to consumers by credit cards. Cash card and credit cards are different, which can be used like currency by the owner of the card. Most credit cards are issued by banks or credit unions. The shape and size specified by the identification cards ISO/IEC 7810 standard as ID-1.

2.2.10.2 History of cards:

In 1987, the concept of card for purchases was described by Edward Bellamy. The modern credit card was the successor of a variety of merchant credit schemes. In United States, it was first used in the 1920s, to sell fuel to a growing number of automobile owners. In 1938, several companies started to accept each other's cards. Charge cards is another type of card begun in Western Union. Some charge cards were printed on paper card stock, but were easily counterfeited.

2.2.10.3 Benefits to customers:

Convenience, is the main benefit to each customer. Compared to debit cards and cheques, a credit card allows small short-term loans to be quickly made to a customer who need not calculate a balance remaining before every transaction, provided the total charges do
not exceed the maximum credit line for the card. Credit cards also provide more fraud protection than debit cards.

The rewards and benefits packages are offered by many cards, such as offering enhanced product warranties at no cost, free loss/damage coverage on new purchases, and points which may be redeemed for cash, products, or airline tickets. Additionally, carrying a credit card may be a convenience to some customers as it eliminates the need to carry any cash for most purposes. [31]

2.2.10.4 Debit Cards:

Like credit card it is also an alternative payment method. A debit card is a plastic card that provides cash when making purchases. Functionally, it can be called an electronic check, as the funds are withdrawn directly from either the bank account or from the remaining balance on the card. In some cases, the cards are designed exclusively for use on the internet, and so there is no physical card.

Majority of countries are using debit cards and it becomes so widespread that their volume of use has overtaken or entirely replaced the cheque. Since using debit card it replaces cash transactions. Like credit cards, debit cards are used widely for telephone and Internet purchases and, unlike credit cards, the funds are transferred immediately from the bearer's bank account instead of having the bearer pay back the money at a later date.

Debit cards may also allow for instant withdrawal of cash, acting as the ATM card for withdrawing cash. Merchants may also offer cash back facilities to customers, where a customer can withdraw cash along with their purchase.

2.2.10.5 Advantages:

- A consumer who is not credit worthy and may find it difficult or impossible to obtain a credit card can more easily obtain a debit card, allowing him/her to make plastic transactions.

- For most transactions, a check card can be used to avoid check writing altogether. Check cards debit funds from the user's account on the spot, thereby finalizing the transaction at the time of purchase and bypassing the requirement to pay a credit card bill at a later date, or to write an insecure check containing the account holder's personal information.

- Like credit cards, debit cards are accepted by merchants with less identification and scrutiny than personal checks, thereby making transactions quicker and less intrusive.
Unlike personal checks, merchants generally do not believe that a payment via a debit card may be later dishonored.

- Unlike a credit card, which charges higher fees and interest rates when a cash advance is obtained, a debit card may be used to obtain cash from an ATM or a PIN-based transaction at no extra charge, other than a foreign ATM fees.

### 2.2.10.6 Disadvantages:

- Use of a debit card is not usually limited to the existing funds in the account to which it is linked, most banks allow a certain threshold over the available bank balance which can cause overdraft fees; if the users transaction does not reflect available balance.

- Many banks are now charging over-limit fees or non-sufficient funds fees based upon pre-authorizations, and even attempted but refused transactions by the merchant (some of which may be unknown until later discovery by account holder).

- Many merchants mistakenly believe that amounts owed can be "taken" from a customer's account after a debit card (or number) has been presented, without agreement as to date, payee name, amount and currency, thus causing penalty fees for overdrafts, over-the-limit amounts if not available causing further rejections or overdrafts and rejected transactions by some banks.

- In some countries debit cards offer lower levels of security protection than credit cards. Theft of the users PIN using skimming devices can be accomplished much easier with a PIN input than with a signature-based credit transaction. However, theft of users' PIN codes using skimming devices can be equally easily accomplished with a debit transaction PIN input, as with a credit transaction PIN input, and theft using a signature-based credit transaction is equally easy as theft using a signature-based debit transaction.

- In many places, laws protect the consumer from fraud much less than with a credit card. While the holder of a credit card is legally responsible for only a minimal amount of a fraudulent transaction made with a credit card, which is often waived by the bank, the consumer may be held liable for thousands of rupees, or even the entire value of fraudulent debit transactions.

    The consumer also has a shorter time (usually just two days) to report such fraud to the bank in order to be eligible for such a waiver with a debit card, whereas with a credit card, this time may be up to 60 days. A thief who obtains or clones a
debit card along with its PIN may be able to clean out the consumer's bank account and the consumer will have no recourse.[32]

2.2.11 INFINET:

The INFINET is a satellite based wide area network using VSAT (Very Small Aperture Terminal) technology. INFINET stands for Indian Financial Network. It was set up by the RBI in June 1999. The hub and the Network Management System of the INFINET are located in the Institute for Development and Research in Banking Technology, (IDRBT) Hyderabad (an institute set up by the RBI). A closed user group of the member banks of the network called the "INFINET User Group" has been formed to resolve issues of common interest on a continuing basis. Among the major applications identified for porting on the INFINET in the initial phase are e-mail, Electronic Clearing Service - Credit and Debit, Electronic Funds Transfer and transmission of Inter-city cheque realisation advices. Later, other payment system related applications as well as Management Information System (MIS) applications are proposed to be operationalised.[33]

2.2.12 BANKNET:

BANKNET provides speed of financial transaction. BANKNET stands for banking network. At present, seven centers viz. Mumbai, Delhi, Calcutta, Madras, Nagpur, Bangalore and Hyderabad set up in 1991 by the RBI, this backbone is meant to facilitate transfer of inter-bank (and inter-branch) messages within India by Public Sector banks who are members of this network. More centres (like Pune, Ahmedabad, Kanpur, Lucknow, Chandigarh, Kochi, Jaipur, Bhopal, Patna, Bhubaneshwar, Thiruvananthapuram, Guwahati, Panaji Jammu etc.) are being brought on the network.

2.2.13 Society for Worldwide Inter-bank Financial Telecommunication (S.W.I.F.T.):

Reliable and expeditious telecommunication facilities are provided by the S.W.I.F.T; for exchange of financial message all over the world. The gateway is in Mumbai and efforts are on to other cities through leased lines/public data network.

For exchanging messages between banks and financial institutions S.W.I.F.T. operates as a worldwide financial messaging network. S.W.I.F.T. also markets software and services to financial institutions. Much of it for use on the SWIFTNET Network, and ISO 9362 bank identifier codes (BICs) are popularly known as "SWIFT codes".

The SWIFT network is used by the majority of international interbank messages. As of September 2010, SWIFT linked more than 9,000 financial institutions in 209 countries.
SWIFT transports financial messages in a highly secure way, but does not hold accounts for its members and does not perform any form of clearing or settlement.

SWIFT does not facilitate funds transfer, rather, it sends payment orders, which must be settled via correspondent accounts that the institutions have with each other. Each financial institution, to exchange banking transactions, must have a banking relationship by either being a bank or affiliating itself with one (or more) so as to enjoy those particular business features. Fundamental operating procedure, rules for liability, were established in 1975 and the first message was sent in 1977.\textsuperscript{[34]}

2.2.14 Electronic Data Interface (EDI):

EDI is a computer-to-computer transfer of details of commercial or administrative transactions using an agreed protocol and standard data structure. EDI can be formally defined as “The transfer of structured data, by agreed message standards, from one computer system to another without human intervention”. EDI standards have been developed in respect of specific messages for transmission of business transactions which are electronic equivalents of commercial invoices, purchase orders, transport bookings and payment instructions etc.

EDI offers the potential for increased payment speed, reduced risk of data loss, and simplified reports that combine patient addenda and billing information. The desire for internal improvement is not the only force motivating the implementation of EDI.

Electronic data interchange (EDI) is the structured transmission of data between organizations by electronic means. It is used to transfer electronic documents or business data from one computer system to another computer system, i.e. from one trading partner to another trading partner without human intervention.

EDI implies a sequence of messages between two parties, either of whom may serve as originator or recipient. The formatted data representing the documents may be transmitted from originator to recipient via telecommunications or physically transported on electronic storage media. It goes on further to say that "In EDI, the usual processing of received messages is by computer only”. Human intervention in the processing of a received message is typically intended only for error conditions, for quality review, and for special situations. For example, the transmission of binary or textual data is not EDI as defined here unless the data are treated as one or more data elements of an EDI message and are not normally intended for human interpretation as part of online data processing.\textsuperscript{[35]}
By improving accuracy and speed of accounting operations, financial electronic data interchange (EDI) can enhance a healthcare organization's cash flow. Banks play a key role in implementing EDI for accounts receivable. [36]

2.2.15 Mobile Banking:

Mobile banking is used for using various banking services like- balance checks, account transactions, payments, credit applications etc. via a mobile device such as a mobile phones. The earliest mobile banking services were offered via SMS. In 1999 first European banks started to offer mobile banking on this platform to their customers. Wireless Application Protocol (WAP) support enabling the use of the mobile banking services. [37]

Provision and availment of banking and financial services are referred by mobile banking; with the help of mobile telecommunication devices. The scope of offered services may include facilities to conduct bank and stock market transactions, to administer accounts and to access customized information.

Mobile Banking can be said to consist of three inter-related concepts:

- Mobile Accounting.
- Mobile Brokerage.
- Mobile Financial Information Services.

Most services are transaction-based, in the categories designated accounting and brokerage. The non-transaction-based services of an informational nature are however essential for conducting transactions - for instance, balance inquiries might be needed before committing a money remittance. The accounting and brokerage services are therefore offered invariably in combination with information services. Information services, on the other hand, may be offered as an independent module.

2.2.15.1 Trends in Mobile Banking:

Due to advance changes in internet it enables new ways to conduct banking business, resulting in the creation of new institutions, such as online banks, online brokers and wealth managers. Such institutions still account for a tiny percentage of the industry.

The mobile and wireless market has been one of the fastest growing markets in the world over the last few years and it is still growing at a rapid pace. With mobile technology, banks can offer services to their customers such as doing funds transfer while travelling, receiving online updates of stock price or even performing stock trading while being stuck in traffic. Smart phones and 3 or 4 or 5 G connectivity provide some capabilities that older text message-only phones do not.
It is believed that mobile users have just started to fully utilize the data capabilities in their mobile phones. In Asian countries like India, China, Bangladesh, Indonesia and Philippines where mobile infrastructure is comparatively better than the fixed-line infrastructure. Also in European countries; where mobile phone penetration is very high (at least 80% of consumers use a mobile phone), mobile banking is likely to appeal even more.

2.2.15.2 Mobile Banking Services:
Mobile banking can offer services such as the following:

- Account Information.
- Mini-statements and checking of account history.
- Alerts on account activity.
- Monitoring of term deposits.
- Access to loan statements.
- Access to card statements.
- Mutual funds/equity statements.
- Insurance policy management.
- Pension plan management.
- Status on cheque, stop payment on cheque.
- Ordering cheque books.
- Balance checking in the account.
- Recent transactions.
- Due date of payment (functionality for stop, change and deleting of payments).
- PIN provision, Change of PIN and reminder over the Internet.
- Blocking of (lost, stolen) cards.

2.2.15.3 Additional Mobile services - Payments, Deposits, Withdrawals and Transfers:

- Domestic and international fund transfers.
- Micro-payment handling.
- Mobile recharging.
- Commercial payment processing.
- Bill payment processing.
- Peer to Peer payments.
- Withdrawal at banking agent.
- Deposit at banking agent.
A specific sequence of SMS messages will enable the system to verify if the client has sufficient funds in his or her wallet and authorize a deposit or withdrawal transaction at the agent. When depositing money, the merchant receives cash and the system credits the client's bank account or mobile wallet. In the same way, the client can also withdraw money at the merchant: through exchanging SMS to provide authorization, the merchant hands the client cash and debits the merchant's account.

III Security in E-banking:

2.3.1 Introduction:

The most complicated challenges that need to be addressed jointly by the bank’s IT departments, mobile application developers and wireless network service providers is security of financial transactions, being executed from some remote location and transmission of financial information.

The following aspects need to be addressed to offer a secure infrastructure for financial transaction over wireless network:

- Physical part of the hand-held device - If the bank is offering smart-card based security, the physical security of the device is more important.
- Security for any device on which clients application running - In case the device is stolen, the hacker should require at least an ID/Password to access the application.
- Authentication of the device with service provider before initiating a transaction. This would ensure that unauthorized devices which are not connected to perform financial transactions.
- Encryption of the data being transmitted over the space.
- Encryption of the data that will be stored in device for later / off-line analysis by the customer.

The latest tool i.e. one time passwords (OTPs) are used by financial and banking service providers in the fight against cyber fraud. Instead of relying on traditional memorized passwords, OTPs are requested by consumers each time they want to perform transactions using the online or mobile banking interface. When the request is received the password is sent to the consumer’s phone via SMS. The password is expired once it has been used or once its scheduled life-cycle has expired.

As the concerns made explicit above, it is extremely important that SMS gateway providers can provide a decent quality of service for banks and financial institutions in regards to SMS services. Therefore, the provision of service level agreements (SLAs) is a
requirement for this industry. So it is necessary to give the bank customer delivery guarantees of all messages, as well as measurements on the speed of delivery, throughput, etc. SLAs give the service parameters in which a messaging solution is guaranteed to perform.

2.3.2 **Scalability and Reliability:**

To scale-up the banking infrastructure to handle exponential growth of the customer base is another challenge for the chief information officer (CIO) and chief technology officer (CTO) of the banks. With E-banking, the customer may be sitting in any part of the world (true anytime, anywhere banking) and hence banks need to ensure that the systems are up and running in a true 24 x 7 fashion. As customers will find E-banking more and more useful, their expectations from the solution will increase. Banks unable to meet the performance and reliability expectations may lose customer confidence. Recently in India there has been a phenomenal growth in the use of E-banking services, with leading banks adopting innovative security techniques.

2.3.3 **Application distribution:**

It would be impractical to expect customers to regularly visit banks or connect to a web site for regular upgrade of their E-banking application; due to the nature of the connectivity between bank and its customers. It will be expected that the internet, mobile application itself check the upgrades and updates and download necessary patches. However, there could be many issues to implement this approach such as upgrade / synchronization of other dependent components.

2.3.4 **Personalization:**

It would be expected from the application to support personalization such as:

- Preferred language.
- Date / Time format.
- Amount format.
- Default transactions.
- Standard Beneficiary list.
- Alerts.

2.3.5 **Software-Based Systems:**

The coding and decoding of information is done using specialized security software, in software-based security systems. Due to the easy portability and ease of distribution
through networks, software-based systems are more abundant in the market. Encryption is the main method used in this software-based security system.

2.3.5.1 Secure Socket Layer (SSL):

Over the internet, the communications security is provided by Transport layer security (TLS) and its predecessor, secure sockets layer (SSL), which are cryptographic protocols. TLS and SSL encrypt the segments of network connections above the transport layer, using symmetric cryptography for privacy and a keyed message authentication code for message reliability.

Several versions of the protocols are in widespread use in applications such as web browsing, E-mail, internet faxing, instant messaging and voice-over-IP.

2.3.5.1.1 Working with SSL:

SSL Overview

All communications between a client and a target system is encrypted by a communication facility i.e. Secure sockets layer (SSL). SSL achieves its security by using certificates to authenticate each side of a connection made between two parties. The certificates allow for the certain identification of those parties and for the negotiation of an encrypted channel for communication. The certificates themselves are files whose alteration can be easily detected and whose origin is verified by a trusted certificate authority. Web browsers use SSL and request SSL certificates from their servers to communicate with online stores, banks, and other service providers. These are the same kind of certificates, but are used for a different purpose. A web browser will typically be verifying the identity of the server and will be contacting a certificate authority to do so.

2.3.5.1.2 Using SSL:

In concert with a certificate authority, a service provider (such as a target system) is authorized to manufacture certificates. The authority can be any entity that the target system trusts including itself. Certificates are delivered to a client system by the target system when the two are negotiating an SSL connection. When starting a connection to a server, it first attempts an SSL connection and then falls back to non-SSL; if the SSL fails.

2.3.5.2 Encryption:

Encryption is a process that modifies information in a way that makes it unreadable until the exact same process is reversed. In general, there are two types of encryption. The
first one is the conventional encryption schemes, one key is used by two parties to both encrypt and decrypt the information. Once the secret key is entered, the information looks like a meaningless jumble of random characters. The file can only be viewed once it has been decrypted using the exact same key.

The second type of encryption is known as Public key encryption is the second type of encryption. In this method, there are two different keys held by the user: a public key and a private key. These two keys are not interchangeable but they are complementary to each other, meaning that they exist in pairs. Therefore, the public keys can be made public knowledge and posted in a database somewhere. Anyone who wants to send a message to a person can encrypt the message with the recipient public key and this message can only be decrypted with the complementary private key. Thus, nobody but the intended receiver can decrypt the message. The private key remains on one’s personal computer and cannot be transferred via the Internet. This key is encrypted to protect it from hackers breaking into the personal computer. There are four examples of current encryption technology viz. Digital Signature, Secure Electronic Transaction, Pretty Good Privacy, and Kerberos.[39][40]

2.3.5.3. Biometric ATMs:

An ATM is a computerized telecommunication device that provided the clients of a financial institution with access to financial transactions in a public space without the need of cashier/clerk. ATMs with biometric devices are the up-to-the minute solution in the ongoing effort to offer banking services, fraud prevention measures, transaction and network security, access control, also offer semi or illiterate folk of rural area to become part of the banking community. Biometric is a method for verifying based on individual’s physical traits. e.g. finger print, palm, facial recognition, hand geometry, iris scan etc. Biometric objects cannot be stolen or hacked, is the advantage of this technology. [41][42][43]

2.3.6 Working of Payment Gateway:

The transfer of information between a payment portal (such as a website, mobile phone) and the front end processor or acquiring bank is facilitated by a payment gateway. When a customer orders a product from a payment gateway-enabled merchant, the payment gateway performs a variety of tasks to process the transaction. These tasks are as follows-

1. A customer places order on website by pressing the 'Submit Order' or equivalent button or perhaps enters their card details using an automatic phone answering service.
2. If the order is via a website, the customer's web browser encrypts the information to be sent between the browser and the merchant's web server. This is done via SSL (Secure Socket Layer) encryption.

3. The merchant then forwards the transaction details to their payment gateway. This is another SSL encrypted connection to the payment server hosted by the payment gateway.

4. The payment gateway forwards the transaction information to the payment processor used by the merchant's acquiring bank.

5. The payment processor forwards the transaction information to the card association (e.g., Visa/MasterCard)

6. The credit card issuing bank receives the authorization request for credit or debit checks and then sends a response back to the processor (via the same process as the request for authorization) with a response code (e.g. approved, denied). In addition to communicating the fate of the authorization request, the response code is used to define the reason why the transaction failed (such as insufficient funds, or bank link not available). Meanwhile, the credit card issuer holds an authorization associated with that merchant and consumer for the approved amount. This can impact the consumer's ability to further spend

7. The processor forwards the authorization response to the payment gateway.

8. The payment gateway receives the response and forwards it on to the website (or whatever interface was used to process the payment) where it is interpreted as a relevant response then relayed back to the merchant and cardholder.

9. The entire process typically takes 2–3 seconds.

10. The merchant then fulfills the order and the above process is repeated but this time to "Clear" the authorization by consummating the transaction. Typically the "Clear" is initiated only after the merchant has fulfilled the transaction (e.g. shipped the order). This results in the issuing bank 'clearing' the 'auth' (i.e moves auth-hold to a debit) and prepares them to settle with the merchant acquiring bank.

11. The merchant submits all their approved authorizations, in a "batch" (e.g. end of day), to their acquiring bank for settlement via its processor.

12. The acquiring bank makes the batch settlement request of the credit card issuer.

13. The credit card issuer makes a settlement payment to the acquiring bank (e.g. the next day).
14. The acquiring bank subsequently deposits the total of the approved funds in to the merchant's nominated account (e.g. the day after). This could be an account with the acquiring bank if the merchant does their banking with the same bank, or an account with another bank.

15. The entire process from authorization to settlement to funding typically takes 3 days.

![Fig. 2.1 Payment Gateway model](http://www.weblinkindia.net/images/pg-process.jpg)

2.3.7 e-fraud cases:

On internet and from customer complaint-reports of RBI, information about many e-fraud cases are found. On its basis, Researcher has taken some references:

2.3.7.1 Retail fraud

In online auction scheme, a fraudster starts an auction on a site such as eBay with very low prices and no reserve price, especially for typically high priced items like watches, computers, or high value collectibles. The fraudster accepts payment from the auction winner, but either never delivers the promised goods or delivers an item that is less valuable than the one offered—for example, a counterfeit or used item.

Online retail schemes involve complete online stores that appear to be legitimate. As with the auction scheme, when a victim places an order through such a site, their funds are taken but no goods are sent, or inferior goods are sent. In some cases, the stores or auctioneers were once legitimate, but eventually stopped shipping goods after accepting customer payments.
Sometimes fraudsters will use phishing techniques to hijack a legitimate member accounts on an online auction site—typically an account with a strongly positive online reputation—and use it to set up a phony online store. In this case, the fraudster collects the money, while ruining the reputation of the conned eBay member. When victims complain that they have not received their goods, the legitimate account holder receives the blame.

### 2.3.7.2 PayPal Fraud

In a collection in person PayPal scheme, the scammer targets eBay auctions that allow the purchaser to personally collect the item from the seller, rather than having the item shipped, and where the seller accepts PayPal as a means of payment.

The fraudster uses a fake address with a post office box when making their bids, as PayPal will allow such an unconfirmed address. Such transactions are not covered by PayPal's seller protection policy. The fraudster buys the item, pays for it via PayPal, and then collects the item from the victim. The fraudster then challenges the sale, claiming a refund from PayPal and stating that they did not receive the item. PayPal's policy is that it will reverse a purchase transaction unless the seller can provide a shipment tracking number as proof of delivery; PayPal will not accept video evidence, a signed document, or any form of proof other than a tracking number as valid proof of delivery.

This form of fraud can be avoided by only accepting cash from buyers; who wish to collect goods in person.

### 2.3.7.3 Call tag scam

In a call tag scam, criminals use stolen credit card information to purchase goods online for shipment to the legitimate cardholder. When the item is shipped, the criminal receives tracking information via email. They then call the cardholder and falsely identify themselves as the merchant that shipped the goods, saying that the product was mistakenly shipped and asking permission to pick it up when it is delivered. The criminal then arranges the pickup, using a "call tag" with a different shipping company. The victim usually doesn't notice that a second shipping company is picking up the product, and the shipping company has no knowledge it is participating in a fraud scheme.

The cardholder may later notice the charge on his statement and protest the charge, generating a chargeback to the unsuspecting merchant.
2.3.7.4 Business opportunity or "Work-at-Home" scams

Con artists often use the Internet to advertise supposed business opportunities that allow individuals to earn thousands of dollars a month in "work-at-home" ventures. These schemes typically require the individuals to pay nominal to substantial sums for the "business plans" or other materials. The fraudsters then fail to deliver the promised materials, provide inadequate information to make a viable business, or provide information readily available for free or a substantially lower cost elsewhere. In one such scheme, after paying a registration fee the victim will be sent advice on how to place ads, similar to the one that recruited him, in order to recruit others.

Another work-at-home scam involves kits for small doodads such as CD cases to be assembled by the victim in their home. The victim pays a fee for the kit, but after assembling and returning the item, the scammer rejects it as substandard, refusing to reimburse the victim for the cost of the kit.

2.3.7.5 Money transfer fraud

Money transfer fraud consists of an offer of employment transferring money to a foreign company, supposedly because it costs too much to do it through other methods. The prospective victim receives an email like these six examples:

Dear Sir/Madam, xxxxxx is a small scale company in xxxxx. We supply xxxxxxx to clients in some countries. We have reached big sales volume in Europe as a starter, and now we are trying to penetrate the US/Canada market. Quite soon we will open representative offices or authorized sales centers in the US and therefore we are currently looking for people who will assist us in establishing a new distribution network there.

The fact that despite the US market is new for us we already have regular clients also speaks for itself. The international money transfer tax for legal entities (companies) in xxxxxx country is 25%, whereas for the individual it is only 7%. There is no sense for us to work this way, while tax for international money transfer made by a private individual is 7%. That's why we need you! We need agents to receive payment for products in money orders, cheque or bank wire transfers and to resend the money to us via Money Gram or Western Union Money Transfer. This way we will save money because of tax decreasing.

**Job description:**
1. Receive payment from Clients
2. Cash Payments at your Bank
3. Deduct 10% which will be your percentage/pay on Payment processed.
4. Forward balance after deduction of percentage/pay to any of the offices you will be contacted to send payment to (Payments are to be forwarded either by Money Gram or Western Union Money Transfer).
**How much will you earn:** 10% from each operation! For instance: If you receive 7000 USD via cheques or money orders on our behalf. You will cash the payment and keep $700 (10% from $7000) for yourself! At the beginning your commission will equal 10%, though later it will increase up to 15%!

**Advantages:** You do not have to go out as you will work as an independent contractor right from your home office. Your job is absolutely legal. You can earn up to $3000–4000 monthly depending on time you will spend for this job. You do not need any capital to start. You can do the work easily without leaving or affecting your present job. The employees who make efforts and work hard have a strong possibility to become managers. Anyway our employee never leaves us.

**Main requirements:** 18 years or older legally capable responsible ready to work 2–4 hours per week with PC knowledge e-mail and internet experience (minimal) And please be informed that Everything is absolutely legal. If you are interested in our offer, please reply to the following email address: xxxxxx@xxxx with your; (1) Your full names: (2) Contact address: (3) Tele/cell numbers: (4) Occupation: (5) Age: (6) Sex: Thanks for your anticipated action. And we hope to hear back from you soon.

**2.3.7.6 Charity fraud**

The scammer poses as a charitable organization soliciting donations to help the victims of a natural disaster, terrorist attack (such as the Sept. 11, World Trade Center attack), regional conflict and the tsunami were popular targets of scammers perpetrating charity scams; other more timeless scam charities purport to be raising money for cancer, AIDS or children's orphanages (the scammer pretends to work for the orphanage or a non-profit associated with it), or impersonates charities such as the Red Cross or United Way. The scammer asks for donations, often linking to online news articles to strengthen their story of a funds drive.

The scammer's victims are charitable people who believe they are helping a worthy cause and expect nothing in return. Once sent, the money is gone and the scammer often disappears, though many attempt to keep the scam going by asking for a series of payments. The victim may sometimes find themselves in legal trouble after deducting their supposed donations from their income taxes.

The scammer may tell the victim their donation is deductible and provide all necessary proof of donation, but the information provided by the scammer is fictional, and if audited, the victim faces stiff penalties as a result of the fraud. Though these scams have some of the highest success rates especially following a major disaster, and are employed by
scammers all over the world, the average loss per victim is less than other fraud schemes. This is because, unlike scams involving a large expected payoff, the victim is far less likely to borrow money to donate or donate more than they can spare.

2.3.7.7. International modem dialing

Customers of dial-up internet service providers, such as aol, use a modem to dial a local telephone number in order to connect to the Internet. Some web sites, typically containing audit content, trick consumers into paying to view content on their web site by convincing them to unwittingly make international telephone calls with their modem.

Often these sites claim to be free, and advertise that no credit card is needed to view the site. They prompt the user to download a "viewer" or "dialer" program to allow them to view the content. Once the program is downloaded, it disconnects the computer from the victim's usual Internet service provider and dials an international long-distance or premium-rate number, charging unexpectedly high rates to the victim's long-distance phone bill.

While one can usually request that their phone company block their line from making international calls in order to prevent this scam, there are loopholes that the scammers can exploit. In the United States and Canada, phone numbers are assigned Country Code "1" and a three-digit "area code" under the north American numbering plan (NANP).

However, bermuda and 16 caribben countries are also part of the NANP, so a phone number that has the same appearance as a domestic number may actually be an expensive overseas call. Scammers can also use a "Carrier Access Code" to override the user's default choice of long-distance company; this works around the international-calling block that the customer placed with that company.

2.3.7.8 Internet marketing and retail fraud

Internet marketing and retail fraud is a fast-growing area perpetrated by dishonest internet marketing and retail sites involving a variety of products and services. The victim is tricked, by a legitimate-looking site and effective marketing, into giving their credit card information and [card security code] (or sending funds by other means) in exchange for what they believe to be goods or services. The goods never arrive, turn out to be fake, or are products worth less than those advertised.

2.3.7.9 Sympathy Fraud Mails

I am writing this mail to you with heavy sorrow in my heart. I want you to carefully go through this mail and let me know if you can handle this project for me so that Allah will
take the glory. So do not be afraid am very honest with my offer. I am contacting you from Burkina-Faso, I tell you this because I don't have any other option than to tell you as i was touched to open up to you.

My name is Mrs Yomun Barakah, i am married to Mr. Asad Barakah, who worked with Tunisian embassy in Burkina-faso for nine years before he died in the year 2005. We were married for eleven years without a child. He died after a brief illness that lasted for only five days. Since his death i decided not to remarry, when my husband was alive he deposited the sum of us$ 8.2m (Eight million two hundred thousand dollars) in a bank in Burkina-faso here west Africa.

Presently this money is still in the bank. He made this money available for exportation of gold from Burkina-faso mining. Recently, my doctor told me that i would not last for the period of seven months due to cancer problem. You see, whosoever that want to serve Allah must serve him in spirit and in truth because Allah is the most high, please always be prayerful all through your live. The one that disturbs me most is my cancer sickness. Having known my condition i decided to hand you over this money to take care of the less privileged people. You will utilise this money the way i am going to instruct you herein. I want you to take 30% of the total money for your personal use while 70% of the money will go to charity, people in the street and helping the orphanage. I don't have any child that will inherit this money and my husband relatives are not good, not even good at all because they are the one responsible for the death of my husband in other to have all my late husband's properties and i don't want my husband's efforts to be used by those that conspired for his death.

I grew up as an orphan and i don't have anybody as my family member. I am doing this so that Allah will forgive my sins and accept my soul when i die, because this sickness has suffered me so much. As soon as i receive your reply assuring me your capability then i shall give you the contact of the bank, and i will send an authority letter to the bank that will prove you as the resent beneficiary of the money in the bank, that is if you assure me that you will act accordingly as i instructed you herein.

Hoping to receive your reply. Mrs Yomun Barakah.

(Ref. Dated, 19-10-12, Yahoo mail)

2.3.7.10 Online Banking Fraud Schemes

Most online banking fraud schemes involve two steps. First, the criminal obtains the customer's account access data, i.e. logon name and password. Second, the criminal uses this information to transfer money to other accounts and withdrawals the funds. For the first step, criminals have employed different schemes in the past. The "over the shoulder looking"
scheme occurs when a customer performs financial transactions while being observed by a criminal.

A fair number of cases have been reported where customer's account access data was obtained by the criminal just by observing customers at a public Internet access point. The "phishing" scheme involves using fake emails and/or fake websites. The word "phishing" stems from combining the words "password" and "fishing". Criminals send emails that appear to be from the customer's bank that direct customers to a fake website.

This website impersonates the bank's website and prompts customers for their account access data. Over the past months, most banks have executed customer education programs, thereby reducing the effectiveness of this scheme. It will, however, take awhile before all customers are smart enough to extinct phishing.

2.3.7.11 Trojan horse scam

The "Trojan horse" scheme is based on embedding a computer virus type software program onto the customer's PC. Trojans often tie themselves into the keyboard driver and record keystrokes. Once a Trojan detects that the customer opens an online banking website, it captures login name and password, and sends it to the criminal.

In the year 2003, Phishing was the dominant fraud scheme. In the year 2004, banks experienced a sharp rise in Trojan fraud scheme attacks.

2.3.8 e-fraud control suggestions:

While online banking has been around for many years, virtually very less cases of fraud have been reported until recently. Since the beginning of the year 2004, reports of fraud cases nearly explode and banks are looking for ways to protect their online banking channel.

2.3.8.1 One Time Passwords

To improve security, some banks use "one time passwords", also called OTP. Upon activation of the customer's account for online banking, the bank mails a list of OTPs to the customer. Each time the customer perform a transaction, he enters one OTP for verification. Once used, the OTP becomes invalid. If the customer runs out of OTPs, he is sent a new list.

While this approach effectively prevents "over the shoulder looking", it generally fails to prevent other fraud schemes. Phishing emails also ask for OTPs, and a customer naive enough to give out his logon name and password will likely also provide OTPs.

Trojans simply also capture the OTP once entered. At the same time, they falsify the customer's input in the browser software (e.g. by adding an invisible character) or cause the browser software to crash. This causes the customer's transaction to be intercepted and the
OTP to still be valid. The criminal can then use this valid OTP to perform a fraudulent transaction.

2.3.8.2 Smart Cards and USB Tokens

Smart cards and USB tokens implement a different approach to authentication. Smart cards contain crypto processors without a display. They must be electrically connected to the customer's PC using a card reader device. USB tokens are essentially the same, only that they render card readers unnecessary by plugging directly into the customer PC's USB port. By exchanging crypto keys with the bank's server, the bank's server can be sufficiently sure that the online transactions secured with this approach stem from the genuine customer. While smart cards have been hacked in the past, the latest generation smart cards will likely provide a high level of fraud protection for many years.

2.3.8.3 Transaction Monitoring

A completely different approach to secure online banking comes from the adaptation of fraud prevention systems used with credit and debit card processing. In payment card processing, fraud is a known phenomenon since many years. Technical security measures introduced to payment cards, such as magnetic stripes or chips, have only provided temporary relief from fraud losses.

The only measure that has proved to limit fraud losses permanently was the deployment of transaction monitoring software. This has become the de-facto standard for fraud prevention with payment card processing worldwide.

Transaction monitoring occurs in the bank's data centre. For each transaction, the transaction monitoring software scrutinizes the current transaction's parameters, and compares it with the previous transaction of both the customer and the counterparty of the transaction histories. By comparing the current transaction pattern to stored known fraud patterns, the software can flag suspicious transactions "on the fly". Such transactions are then referred to a call centre for manual verification.

There are multiple advantages to this approach when compared to the others discussed before. There is no new device to be used by the customer, no dependency on mobile phones and no customer support problem with hardware driver installation. There are also no one-time costs per customer for a card reader or an USB token, and no per-transaction cost for sending SMS.
2.3.8.4 RiskShield Fraud Prevention

Inform Software Corp has recently introduced a special version of RiskShield for online banking. This product is currently in rollout with online banking operations of 3 major European banks.

RiskShield is delivered with countermeasures against all known online banking fraud patterns. A fraud pattern for example can be an unusually high frequency of payments going into one target account from different source account. If none of the source accounts have ever transferred funds to this target account before, and the transactions have all been originated from IP address ranges belonging to certain Internet service providers never used before by the source account holders, RiskShield will conclude that this is part of a fraud scheme and will refer transactions to the call centre. At the moment, RiskShield's prevention logic contains about 80 different online banking fraud patterns plus variants.

In addition, RiskShield looks out for "unusual" transaction patterns because they could be emerging fraud patterns. Once RiskShield administrators are alerted, they use the RiskShield analysis and simulation environment to isolate potentially new fraud patterns, and simulate the effectiveness of the developed countermeasures.

RiskShield also uses transaction data from other payment channels to refine its detection of certain fraud patterns, if such data is available. The transaction sequences are automatically merged by RiskShield into "transaction fingerprints". Also, non-monetary transactions, such as password changes, address changes or claims of lost cards are used by RiskShield to detect specific fraud patterns.

2.3.8.5 Cyber crime and IT Act 2000:

With the advent of E-banking in the country, number of online frauds and cyber criminals have gone up. Cyber criminals misuse the lack of knowledge among users and use technology loopholes to conduct their crime and cheat the public of its money. They uses various means like hacking, fake websites and spam mails, and convey to the customers for giving banking details. Once PIN or secret number or password identified then it is used to carry out transactions on their behalf without their knowledge. With the changing technology, it becoming more difficult to control such frauds due to problems in collection of digital evidence, attribution of attacks to particular systems, anonymous and border less nature of cyber space.

Section 43 and 43A of the Information Technology (IT) Act, 2000 provides for compensation for the damages suffered by the victims of computer crimes and frauds. Section
66 and Section 72A provides punishment in the form of imprisonment and fine to the person behind it.

Cyber crimes are reduced by providing training on cyber security, best practices, cyber forensics to people at different levels like general public, law enforcement agencies and judicial officers. Further there is also an urgent need to increase the training infrastructure and the number of trainers in the country so that sufficient awareness about cyber security can be generated, which will help in preventing cyber attacks.

2.3.9 Foreign currency exchange and E-banking:

Foreign exchange facility helps to service users for converting currencies in to different other countries currency. Foreign Exchange Online provides simplicity and convenience right at your fingertips. It is a smart, simple and secure solution that puts you in control of your foreign exchange transactions. No line-ups. No calling and waiting for a rate quote. No more hassles.

Foreign exchange online follows some specific conditions these are:

- User must be a business client with accounts at service banks providing foreign exchange.
- User must have a minimum yearly foreign exchange requirement.

Foreign exchange Online Key Benefits:

- Obtain real time, competitive exchange rates with currencies.
- Choose from a range of currency products from spot and swaps to open and fixed dated forward contracts.
- Receive foreign currency wires, convert them online and credit your account.
- Order foreign currency wires, send drafts, and transfer funds between accounts, all in one transaction from your desktop.

Services

- Create templates for recurring payments or settlement instructions.
- Confirm and settle trades online whether booked by telephone or online.
- Receive e-mail alerts of outstanding trades or settlements.
- Create customized reports of your transactions which can be exported to a file for your use.

Security

- Separate trading and settlement users for additional security is provided by bank.
- Set up settlement limits or restrict payment methods for safe delegation of work.
Easy access to support via e-mail, telephone or online help.

2.4 Conclusion:

Electronic banking is offering its customers with a wide range of services. Customers are able to interact with their banking accounts as well as make financial transactions from virtually anywhere without time and restrictions. Electronic Banking is offered by many banking institutions due to pressures from competitions. To add further convenience to the customers, many banking institutions are working together to form an integrated system such as the Integration Financial Network and the Gendex Bank International. In order to continuing of electronic banking’s growth, the security and the privacy aspects need to be improved. With the security and privacy issues resolved, the future of electronic banking can be very prosperous. The future of electronic banking will be a system where users are able to interact with their banks “worry-free” and banks are operated under one common standard.

To study the conceptual framework is one of the objectives of this research. This objective is fulfilled by studying the various concepts used while using E-banking services.

References

36. E-Procurement-Electronic Data Integration Comes of Age, Article from Finance Director Europe Journal, accessed on 17 aug 2011.