Chapter – 3

E-BANKING,

E-PAYMENTS AND

E-FRAUDS
3.1 E-BANKING

3.1.1 Introduction to E-banking

The Indian economy has been driven by the year 1991 liberalization policies that have been instrumental in boosting demand as well as trade volume. The Gross Domestic Product (GDP) in India expanded 8.20 percent in the fourth quarter of 2010 over the same quarter, 2009. From 2004 until 2010, India's average quarterly GDP growth was 8.40 percent reaching an historical high of 10.10 percent in September of 2006 and a record low of 5.50 percent in December of 2004.

With the rapid globalization of the Indian economy during early 1990s, the banking and financial institutions faced increased competition in an ever changing environment. These banking and financial institutions adopted strategies aimed at developing competitive advantage based on enhanced customer value in terms of product differentiation, quality, speed, service and costs. The deregulation and adoption of technology led to a revolution in the banking Industry. Banks have become global industrial powerhouses that have created ever more complex products. Through technology development, banking services have become available 24x7 through ATMs, at online banking, and in electronically enabled exchanges where everything from stocks to currency futures contracts (Foreign exchange future or FX future) can be traded.

E-banking services are delivered to customers through the internet and the web using Hypertext Markup Language (HTML), XML, PHP, Ruby, and Python. In order to use E-banking services, customers need internet access and web browser software. Multimedia information in HTML format from online banks can be displayed in web browsers. The heart of the E-banking application is the computer system, which includes web servers, database management systems, and web application programs that can generate dynamic HTML pages. It is as shown in the diagram (Figure 3.1)
In the post liberalization era, with the deregulation of Indian economy, the financial service sector witnessing a complete metamorphosis with adoption of latest technology (web technology). The past two decades have witnessed enormous reductions in the cost of information technology. Between 1986 and 1995, the computing power of the average PC increased eleven folds while the price declined. At the same time, a revolution in telecommunications reduced the cost of transmitting data by 90 percent since 1980. Such cost reductions have made it ever less expensive to acquire, store, transmit, and transform data into information. They have also created enormous changes in data-intensive industries such as financial services. Over the last decade India has been one of the fastest adopters of information technology, particularly because of its capability to provide software solution. To name a few - Infosys’s - Finacle, Iflex’s - Flexcube software to organizations around the world. This capability has provided a tremendous impetus to the domestic banking industry in India to deploy the latest in technology, particularly in the Internet banking and E-commerce areas. Most of the banks started computerization of core banking areas in 2000. In 2006 77.5 % of the branches were fully computerized and by 2010, banks in India achieved 100% computerization in 97% branches. (RBI report, 2010).

According to 2009 RBI report, 27 public sector banks cumulatively spent Rs 17,897 crores on computerization and development of communication networks between September 1999 and March 2009. The proportion of public sector bank (PSB) branches that achieved full computerization has increased from 93.7 per cent at March-end 2008 to 95 per cent at March-end 2009. Technology is playing a major role in increasing the efficiency, courtesy and speed of customer service. An online banking user is expected to perform at least one of the following transactions online.
like checking account balance and transaction history, paying bills, transferring funds between accounts, requesting credit card advances, ordering checks and managing investments and stocks trading. As speedier Internet arrived in India and so its usage as more and more banks started offering e-banking services. In 2009, due to introduction of broadband communications by major Internet Service Provider (ISP) s, internet penetration has also increased.

3.1.2 Internet penetration

Currently the penetration of technology in terms of internet in India is very low. It is just 8.5% (as mentioned in Table 3.1) in India with just 121 million people hooking to the online facility. A minor part of this segment is aware and uses the internet banking facility. Even in this small segment there is a resistance towards adopting the technology based services like banking on the internet due to lack of confidence in security of their data.

<table>
<thead>
<tr>
<th>YEAR</th>
<th>Users</th>
<th>Population</th>
<th>% Pen.</th>
<th>Usage Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>1998</td>
<td>1,400,000</td>
<td>1,094,870,677</td>
<td>0.1%</td>
<td>ITU</td>
</tr>
<tr>
<td>1999</td>
<td>2,800,000</td>
<td>1,094,870,677</td>
<td>0.3%</td>
<td>ITU</td>
</tr>
<tr>
<td>2000</td>
<td>5,500,000</td>
<td>1,094,870,677</td>
<td>0.5%</td>
<td>ITU</td>
</tr>
<tr>
<td>2001</td>
<td>7,000,000</td>
<td>1,094,870,677</td>
<td>0.7%</td>
<td>ITU</td>
</tr>
<tr>
<td>2002</td>
<td>16,500,000</td>
<td>1,094,870,677</td>
<td>1.6%</td>
<td>ITU</td>
</tr>
<tr>
<td>2003</td>
<td>22,500,000</td>
<td>1,094,870,677</td>
<td>2.1%</td>
<td>ITU</td>
</tr>
<tr>
<td>2004</td>
<td>39,200,000</td>
<td>1,094,870,677</td>
<td>3.6%</td>
<td>C.I. Almanac</td>
</tr>
<tr>
<td>2005</td>
<td>50,600,000</td>
<td>1,112,225,812</td>
<td>4.5%</td>
<td>C.I. Almanac</td>
</tr>
<tr>
<td>2006</td>
<td>40,000,000</td>
<td>1,112,225,812</td>
<td>3.6%</td>
<td>IAMAI</td>
</tr>
<tr>
<td>2007</td>
<td>42,000,000</td>
<td>1,129,667,528</td>
<td>3.7%</td>
<td>IWS</td>
</tr>
<tr>
<td>2009</td>
<td>81,000,000</td>
<td>1,156,897,766</td>
<td>7.0%</td>
<td>ITU</td>
</tr>
<tr>
<td>2010</td>
<td>100,000,000</td>
<td>1,173,108,018</td>
<td>8.5%</td>
<td>IWS</td>
</tr>
</tbody>
</table>

The percentage internet penetration in 2000 was very low (0.5%) and with introduction of broadband communications with private ISP’s participation
like TATA, Reliance, Airtel, Idea, MTS, Uninor etc., the percentage rose to 8.5% as shown in Table No3.1, this is far below USA and Japan's population penetration percentage of 75%. Before analyzing the impact of internet on banking industry let us study the computerization and evolution of e-banking in India.

3.1.3 Early phase of E-banking
The Dr. C Rangarajan committee report in the early 1980s was the first step towards computerization of banks. This phase introduced many products and facilities in the banking sector as part of its reforms measure. In 1991, under the chairmanship of M. Narasimham, a committee was set up by his name which worked for the liberalization of banking practices. Efforts are being put to give a satisfactory service to customers. Phone banking and net banking were introduced. The entire system became more convenient and swift. Time is given more importance than money. Thus online banking/E-banking has arrived to serve technology savvy customers.

3.1.4 E-banking
The banking has been defined in the Banking Regulation Act as “the activity of acceptance of deposits of money from the public repayable on demand or otherwise for the purpose of lending or for investment”. Banking has come a long way from the time of ledger cards and other manual filing systems due to computerization.

3.1.5 E-banking definition
The term Internet Banking or E-Banking Internet both are used as synonymous. E-Banking is one of the major parts of E-Financing. E-Banking is web-based banking. In other words E-Banking refers to the banking operations, which is done over World Wide Web (www). However, more comprehensive and well-established definition is given by the United Nations Conference on Trade and Development (UNCTAD). This definition covers almost all area of E-Banking.

Internet banking refers to the deployment over the Internet of retail and wholesale banking services. It involves individual and corporate clients, and
includes bank transfers, payments and settlements, documentary collections and credits, corporate and household lending, card business and some others.

E-Banking is defined as the automated delivery of new and traditional banking products and services directly to customers through electronic, interactive communication channels. E-Banking includes the systems that enable financial institutions, individuals or businesses, to access accounts, transact business, or obtain information on financial products and services through a public or private network, including the Internet. Customers access E-Banking services using an intelligent electronic device, such as a personal computer (PC), personal digital assistant (PDA), automated teller machine (ATM), Kiosk, or Touch Tone telephone. E-Banking involves the handling of an account or a savings book, etc. via electronic media. The figure 3.2 shows the relationship between e-commerce and e-banking.

![Diagram showing the relationship between e-commerce and e-banking](image_url)

**Figure No 3.2: E-Commerce-E-Banking relationship**
3.1.6 E-banking - a historic perspective

E-banking made its debut in UK and USA in the 1920s. It became prominently popular during 1960, through electronic funds transfer and credit cards. The concept of web-based banking came into existence in Europe and USA in the beginning of 1980. The evolution of e-banking started from the use of Automatic Teller Machines (ATMs) and telephone banking (tele-banking), direct bill payment, electronic fund transfer and the revolutionary online banking. The future of electronic banking would be more interactive i.e., TV banking. Finland is the first country in the world to have taken a lead in e-banking. In India, ICICI Bank initiated e-banking services during 1997 under the brand name ‘Infinity’.

In 2007, 95% of Indian banks were computerized and all the nationalized banks are adopted e-banking and mobile banking after achieving 100% computerization of core banking. Most banks today have Electronic systems to handle their daily voluminous tasks of information retrieval, storage and processing. Irrespective of whether they are automated or not, banks by their nature are continually involved in all forms of information management on a continuous basis.

3.1.7 E-banking and ATMS in India

E-banking is a generic term for delivery of banking services and products through electronic channels, such as the telephone, the internet, the cell phone, etc. The concept and scope of E-banking is still evolving. It facilitates an effective payment and accounting system thereby enhancing the speed of delivery of banking services considerably. While E-banking has improved efficiency and convenience, it has also posed several challenges to the regulators and supervisors. Several initiatives taken by the government of India, as well as the Reserve Bank of India (RBI), have facilitated the development of E-banking in India. The government of India enacted the IT Act, 2000, which provides legal recognition to electronic transactions and other means of electronic commerce. The RBI has been preparing to upgrade itself as a regulator and supervisor of the technologically dominated financial system. It issued guidelines on risks and control in computer and telecommunication system to all banks, advising them to evaluate the risks.
inherent in the systems and put in place adequate control mechanisms to address these risks. The existing regulatory framework over banks has also been extended to E-banking. It covers various issues that fall within the framework of technology, security standards, and legal and regulatory issues.

According to RBI-2009 report, as of March-end 2009 out of the 27 PSBs, 15 have put their branches on the 100% core banking solution (CBS) platform. These banks are Andhra Bank, Corporation Bank, Indian Bank, Oriental Bank of Commerce, Punjab National Bank, Syndicate Bank, Union Bank of India, Vijaya Bank, State Bank of India and its six associate banks.

Banks that may need to step up the pace of putting their branches on CBS include Punjab and Sind Bank (1.1 per cent of the total branches on CBS), Allahabad Bank (9.7 per cent), Central Bank of India (30.8 per cent), and Canara Bank (38.6 per cent) as of 2009.

CBS enables banks to automate their core operations through integration of communication and information technology. This platform allows a bank’s customer to operate accounts from any branch of the bank, via internet and mobile phone.

The total number of branches of public sector banks which have implemented CBS increased from 35,464 as on March-end 2008 to 44,304 as on March-end 2009. The process of computerization of the banking sector, which is regarded as the precursor to other technology initiatives, is almost on the completion stage (RBI report-2009).

During 2008-09, banks (public sector, old private sector, new private sector, and foreign) collectively set up 3,479 branches (4,087 in 2007-08) and 8,862 ATMs (7,701 in 2007-08). As on March-end 2009, the number of branches and ATMs of scheduled commercial banks stood at 27,164,608 and 43,651 respectively.

In 2008-09, the number of ATMs as a percentage of branches increased. It was 40.2 per cent for nationalized banks; 56.9 per cent for old private sector banks; and 296.6 per cent for new private sector banks. In the case of the State Bank Group and Foreign banks, the number of ATMs as a percentage of branches declined to 29 per cent and 357.3 per cent respectively.
Of all the ATMs installed in the country as at March-end 2009, new private sector banks had the largest share in off-site ATMs (7,480), while nationalized banks had the largest share in on-site ATMs (10,233). The ATMs are the product of computer and broadband communications offering all the bank services at cost effective manner.

With advent of Automatic Teller Machines (ATM), banks are able to serve customers outside the banking hall. Furthermore, computers help banks to reduce the cost of doing business. The cost of bank transactions from a branch office has come down from ₹ 1.11 to 27 paisa through ATM. Although, the effectiveness of the Information Technology deployment in banks is another matter, the fact remains that IT usage is now a reality with hardware cost and software development cost coming down in this competitive computer world. This is to be expected in view of the huge amount of information being handled by banks on a daily basis. On the customer's side, cash is withdrawn or deposited, cheques are deposited or cleared, statement of accounts are produced, etc. At the same time, banks need up-to-date information on accounts, credit facilities, interest, deposits, charges, income, profitability indices and other financial control information. This calls for a robust e-banking architecture.

3.1.8 E-banking architecture

IT investment by banks include IT infrastructure such as Hardware, Software and Networking (Local, Wide Area and the internet). For E-banking to be effective these areas must be well managed. Banking software can be described as the heart and soul of a bank's IT infrastructure.

But having good banking software may be of little value if hardware is inadequate to meet needs of the banks volume of transactions. Likewise in today's E-banking, Networking cannot be ignored. With the advent of broadband communications with minimum 10 Mbps speed and its acceptance by business sector as well as domestic sector the E-banking has become a reality.
3.1.9 Architecture of e-banking

The E-Banking Application is based on 3-tier model. The Enterprise architecture for E-Banking Application is shown in the figure 3.3.

The 3-tier architecture shown in figure 3.3 has the following major components:

**Client:** There will be two clients for the application. One will be a web-based user-friendly client called bank customers. The other will be for administration purposes.

**Application Server:** It takes care of the server script, JDBC-ODBC driver, and checks for the ODBC connectivity for mapping to the database in order to fulfill client and administrator's request.

**Database:** Database Servers store customer’s and bank data.
The application works based on a request/response protocol. A client initiates a request to the server. The server responds by executing the business logic hosted inside the JSP program and if required, communicates with the Database Server to fulfill a client’s request. This e-banking architecture has lead to many benefits.

3.1.10 Benefits of E-banking

The benefits of Electronic banking encompass a broad range of functions and it includes:

Electronic mail (e-mail) that improves communication between individuals and the bank, within the bank, with the bank and external parties and between banks. The availability of online information provides bankers and customers with a powerful mode of communication.

Banks can provide the desired information and services online for the customers. Banking processes are made more efficient and cost effective by integrating other aspects of banking operations such as treasury management and financial control. If a banking function does not require physical interaction, it may derive the benefits of electronic banking.

Most current E-banking applications use the internet. The advantages of online banking are in providing convenience and flexibility for customers.

Online banking allows customers to get account balances at any time. Customers need not worry whether a cheque has been cleared or a deposit has been posted. At the click of a button, customers can easily check the status of their current, savings, and money-market accounts. Through online banking, banks can provide information of accounts instantly. For customers, Customers need not wait till month end for historical, snail-mail statements.

Online banking gives the ability to pay bills electronically. Electronic payments can be credited the without any delay. Customers can also download account transactions online. It facilitates to import the transactions directly into typical PC programs at home or office.

The transfer of money between accounts is another powerful application of online banking. Online banking provides flexibility, by allowing the customer to access his finances from any part of the globe.
In the present evolving e-climate, it involves using the internet to exploit new opportunities by transforming products and markets, and business processes.

E-banking also means developing new relationships with customers, regulatory authorities, suppliers, and banking partners with digital tools. For example, it requires an understanding that customer/bank relationships will be more personalized, resulting in novel modes of transaction processing and service delivery.

IT today, E-business, E-commerce is not about routine information management or automation. It is about using these unique tools to create opportunities, create new markets, new processes and the creation of e-wealth.

For E-banking to be effective, an area that must be addressed is security. For any IT based service, the convenience associated with E-banking increases the need for security.

In E-banking, the core security areas that must be addressed are confidentiality, integrity and availability. A key concern is that of privacy. One cannot expect to do business on the net without addressing the privacy concerns of customers who do business with the bank. Security in online banking is typically provided through the use of a user ID and password. These and other security measures must be installed and must be effective to prevent not only the breach of privacy, but other security concerns like the alteration of data, IT fraud, etc.

In ensuring system availability banks still have a lot of work to do. When customer apt for e-banking, banking services are totally dependent on IT. In an environment where telecommunication services are still at best epileptic there is a need for powerful and functional programs with good recovery procedures. Fault tolerance and robustness of the IT setup in a bank must never be underestimated. Contingency plans should be put in place to handle this persistent problem of availability.

As E-Banking offering worldwide services, the fault-tolerance of its IT infrastructure cannot be compromised. Availability planning must address power supply, telecommunications, internet service, quality of technical
support, backup facilities and robustness of IT setup (Hardware, banking software, Networking).

E-banking is changing the banking industry and is having the major effects on banking relationships. Banking is now no longer confined to the branches where one has to approach the branch in person, to withdraw cash or deposit a cheque or request a statement of accounts. In true Internet banking, any enquiry or transaction is processed online without any reference to the branch (anywhere banking) at any time. Providing E-banking is increasingly becoming a necessity than “nice to have” service. The E-banking, thus, now is more of a norm rather than an exception in many developed countries due to the fact that it is the cheapest way of providing banking services.

3.1.11 E-banking versus traditional banking

In spite of many facilities that E-banking/ internet banking offers, the customer still seem to trust traditional method of banking and are reluctant to use online banking. But here are a few cases discussed shows why internet banking will turn out to be a better option in terms of saving time and money.

'Stop payment' done through Internet banking will not cost any extra fees but when done through the branch, the bank may charge you Rs 50 per cheque plus the service tax.

Through Internet banking, customer can check his transactions at any time of the day, and as many times as he wants depending on his requirement. On the other hand, in a traditional method, one can get quarterly statements from the bank and if customer request for a statement at his required time, it may turn out to be an expensive affair. The branch may charge about ` 25 per page, which includes only 30 transactions. Moreover, the bank branch might take approximately eight days to deliver it at customer doorstep.

If the fund transfer has to be made outstation, where the bank does not have a branch, the bank would demand outstation charges. Whereas with the help of online banking, it will be absolutely free for the customer.

As per the Internet and Mobile Association of India’s report on online banking 2006, “There are many advantages of online banking. It is
convenient, it isn't bound by operational timings, there are no geographical barriers and the services can be offered at a miniscule cost." The banks in India to serve the customer better and due to RBI initiative in adoption of ICT, banks are starting offering online banking services. Table 3.2 shows the list of banks offering e-banking services in India.

Table 3.2: SAMPLE LIST OF BANKS OFFERING E-BANKING IN INDIA

<table>
<thead>
<tr>
<th>Bank Name</th>
<th>Technology Vendor</th>
<th>Service offering</th>
</tr>
</thead>
<tbody>
<tr>
<td>ABN AMRO Bank</td>
<td>Infosys (Bank Away)</td>
<td>Net Banking</td>
</tr>
<tr>
<td>Abu Dhabi Commercial Bank</td>
<td>Infosys (Bank Away)</td>
<td>ADCB NetLink</td>
</tr>
<tr>
<td>Bank of India</td>
<td>I-flex</td>
<td>BOIonline</td>
</tr>
<tr>
<td>Citibank</td>
<td>Orbitech (now Polaris)</td>
<td>Citibank Online</td>
</tr>
<tr>
<td>Corporation Bank</td>
<td>I-flex</td>
<td>CorpNet</td>
</tr>
<tr>
<td>Deutsche Bank</td>
<td></td>
<td>db direct</td>
</tr>
<tr>
<td>Federal Bank</td>
<td>Sanchez</td>
<td>FedNet</td>
</tr>
<tr>
<td>HDFC Bank</td>
<td>i-flex/Satyam</td>
<td>Net Banking</td>
</tr>
<tr>
<td>HSBC</td>
<td></td>
<td>Online@hsbc</td>
</tr>
<tr>
<td>ICICI Bank</td>
<td>Infosys, ICICI Infotech</td>
<td>Infinity</td>
</tr>
<tr>
<td>IDBI Bank</td>
<td>Infosys (Bank Away)</td>
<td>i-net banking</td>
</tr>
<tr>
<td>IndusInd Bank</td>
<td>CR2</td>
<td>IndusNet</td>
</tr>
<tr>
<td>Punjab National Bank</td>
<td>Infosys (Bank Away)</td>
<td>Internet Banking</td>
</tr>
<tr>
<td>Standard Chartered Bank</td>
<td>In-House</td>
<td>Me Standard Chartered</td>
</tr>
<tr>
<td>State Bank of India</td>
<td>Satyam/Broadvision</td>
<td>onlinesbi.com</td>
</tr>
<tr>
<td>UTI Bank</td>
<td>Infosys (Bank Away)</td>
<td>I connect</td>
</tr>
</tbody>
</table>

The changes in banking regulations have eased this transition toward e-banking, as has the emergence of technologies that enable new competitors to enter the financial services market quickly and efficiently. In fact, it is estimated that only 8% of India’s banks currently offer advanced transactional capabilities, such as cash management services and online fund
transfers. Compared to India’s nationalized banks, private and foreign banks in India are far more advanced in terms of the number of e-banking sites and services available, as well as the level of technological advancement available on these sites.

3.1.12 E-banking operational issues

Financial institutions, their card associations, and vendors are working to develop an Internet payment infrastructure to help make electronic commerce secure. Many in the banking industry expect significant growth in the use of the Internet for the purchase of goods and services and electronic data interchange. The banking industry also recognizes that the Internet must be secure to achieve a high level of confidence with both consumers and businesses.

Sound management of banking products and services, especially those provided over the Internet, is fundamental to maintaining a high level of public confidence not only in the individual bank and its brand name but also in the banking system as a whole. Key components that will help maintain a high level of public confidence in an open network environment include:

- Security
- Authentication
- Trust
- Non-repudiation
- Privacy
- Availability

Security is an issue in Internet banking systems. The office of the comptroller of currency (OCC) expects national banks to provide a level of logical and physical security commensurate with the sensitivity of the information and the individual bank’s risk tolerance.

Firewalls are frequently used on Internet banking systems as a security measure to protect internal systems and should be considered for any system connected to an outside network. Firewalls are a combination of hardware and software placed between two networks through which all traffic must
pass, regardless of the direction of flow. They provide a gateway to guard against unauthorized individuals gaining access to the bank's network.

Authentication is another issue in an Internet banking system. Transactions on the Internet or any other telecommunication network must be secure to achieve a high level of public confidence. In cyberspace, as in the physical world, customers, banks, and merchants need assurances that they will receive the service as ordered or the merchandise as requested, and that they know the identity of the person they are dealing with.

Trust is another issue in Internet banking systems. As noted in the previously, public and private key cryptographic systems can be used to secure information and authenticate parties in transactions in cyberspace. A trusted third party is a necessary part of the process. That third party is the certificate authority.

A certificate authority is a trusted third party that verifies identities in cyberspace. Some people think of the certificate authority functioning like an online notary. The basic concept is that a bank, or other third party, uses its good name to validate parties in transactions. This is similar to the historic role banks have played with letters of credit, where neither the buyer nor seller knew each other but both parties were known to the bank. Thus the bank uses its good name to facilitate the transaction, for a fee.

Non-repudiation is the undeniable proof of participation by both the sender and receiver in a transaction. It is the reason for which the public key encryption was developed, i.e., to authenticate electronic messages and prevent denial or repudiation by the sender or receiver. Although technology has provided an answer to non-repudiation, cyber laws are not uniform in the treatment of electronic authentication and digital signatures. The application of cyber laws to these activities is a new and emerging area of the law.

Privacy is a consumer issue of increasing importance. National banks that recognize and respond to privacy issues in a proactive way make this a positive attribute for the bank and a benefit for its customers. Public concerns over the proper versus improper accumulation and use of personal information are likely to increase with the continued growth of electronic commerce and the Internet. Providers who are sensitive to these concerns have an advantage over those who do not.
Availability is another component in maintaining a high level of public confidence in a network environment. All of the previous components are of little value if the network is not available and convenient to customers. Users of a network expect access to systems 24 hours per day, seven days a week.

Among the considerations associated with system availability are capacity, performance monitoring, redundancies, and business resumption. National banks and their vendors who provide Internet banking products and services need to make certain they have the capacity in terms of hardware and software to consistently deliver a high level of service.

In addition, performance monitoring techniques will provide management with information such as the volume of traffic, the duration of transactions, and the amount of time customers must wait for service. Monitoring capacity, downtime, and performance on a regular basis will help management assure a high level of availability for their Internet banking system.

3.2 E-PAYMENTS

3.2.1 Introduction electronic payment

Today’s societies have recognized information and knowledge as invaluable resources which are very essential element for better living conditions... The ‘agricultural age’, the period when majority of workers were farmers, and 18th century’s ‘industrial age’, the period when work processes were simplified through mechanization and automation, had to pass before the advent of the present 20th century’s ‘information age’. The information age began in the 1960s when majority of people are involved in the creation, distribution, and application of information. The developed countries came through the two preceding ages to reach the information age.

During second generation of computers, the internet became a reality to share the data/information among organizations; information has become a production asset or an input like natural resources, labor, capital, and entrepreneurship. It is unique from other resources in the sense that it can be used, reused, processed, shared, and exchanged without losing value.
The astonishing growth and sophistication of information and communication technology (ICT) is changing societies' ways of life in various parts of the world. One of the leading areas where this is manifested is the way business is conducted. The growth of the internet and World Wide Web (WWW) has made electronic commerce (e-commerce) possible. E-commerce in its simplest sense is trading electronically. It offers consumers and merchants convenience and speed. The success and growth of e-commerce, however, depends on efficient electronic payment (e-payment) system. The slogan ‘no e-payment, no e-commerce’ witnesses the importance of e-payment for e-commerce. E-payment, the transfer of value electronically, in turn depends on secure ICT infrastructure, efficient legal and regulatory regime, and widespread awareness among the public and business.

3.2.2 History of e-payment

In 1918, electric money was born when Federal Reserve Banks first moved currency via telegraph. However it wasn’t until the automated clearinghouse (ACH) was setup by the US Federal Reserve in 1972 that electronic currency became widespread. This provided the US Treasury and commercial banks with an electronic alternative to processing cheques.

In 1939, a serial inventor by the name Luther George Simjian created the Bankmatic automatic teller machine. He filed 20 patents and asked the company now known as Citicorp to test the device. After six months the bank had reported that there was no demand for such a product. However in 1968, Don Wetzel, Tom Barnes (mechanical engineer) and George Chastin (electrical engineer) conceptualized what is now known as the modern ATM. In 1969, the first prototype of the modern ATM was made and patents were then issued in 1973. The first working ATM was installed into the Chemical Bank based in New York City.

The first ATM’s were offline machines, meaning that the money was not automatically withdrawn from users’ accounts. Therefore only exclusive customers with good credit history were able to use ATMs. Today, almost everyone has access to these devices and there were over 4,03,000 ATMs in the US alone. These ATMs now perform over 1.1 billion transactions per month or 26,000 transactions a minute.
Charge cards date back to as early as 1914 when Western Union provided metal cards, allowing deferred payment privileges to preferred customers. These cards were colloquially known as “metal money”. By 1924, General Petroleum Corporation was allowing customers to use metal money to buy petrol/diesel.

In the late 1930s, American Telephone and Telegraph (AT&T) introduced the “Bell System Card” and before long, railroads and airlines had introduced similar cards.

In 1950, Diners Club issued the first “plastic money” charge card and in 1951 it issued the first credit card to 200 customers who could use it at 27 different restaurants in New York. Bank of America issued the BankAmericard (now Visa) the first bank credit card - later in 1958. This was first promoted to traveling salesmen. By the early 1960s, more companies offered credit cards, advertising them as a time-saving device rather than a form of credit. But it wasn't until the establishment of standards for the magnetic strip in 1970 that the credit card became part of the information age. This saw companies such as American Express and MasterCard became huge successes overnight, which prompted moves by US government. To begin regulation of the credit card industry by banning practices such as the mass mailing of active cards to those who had not requested them.

In 1983, RSA encryption algorithm was invented by Ronald Rivest, Adi Shamir and Len Adelman, (hence the name RSA) at Massachusetts Institute of Technology's (MIT) Laboratory for Computer Science. The breakthrough was that it allowed for encryption in a multi-user environment, that is, no active participation was necessary between the sender and the receiver of data at the other end.

3.2.3 Electronic money

The roots of electronic money can be found in the increased use of computers. In 1860, the Western Union introduced the electronic fund transfer (EFT) and this marked the beginning of electronic money. Semi-Automatic Business Research Environment (SABRE) was jointly created by IBM and American Airlines. In 1964, a fully operational airline reservation system, with a real time transaction processing system, was set up by SABRE. The
telephone lines were connected to the terminals fitted at the airport and reservations were done on the basis of credit, for the first time in history. In 1970, all branches of the banks in Europe were linked using mainframes mainly from IBM. France witnessed the use of electronic money, with the introduction of the Mintel services. The French Mintel terminals were given free of cost to everybody so that they could use these terminals for online shopping.

In late 1990s, the technologies related to electronic money like electronic cheques and embedded smart cards used the public key cryptography for transferring money. With the advent of e-mail, the transactions of electronic money started increasing. People started sending their credit card details via e-mail to buy goods. Later, the customers started having an online account to avoid transaction fees.

Nowadays, the use of electronic money is possible due to cryptography and digital signatures. Public key encryption and decryption together are called public key cryptography. The public key encryption involves two keys, viz. public key and private key to authenticate the identity of an entity, electronically. As the name suggests, the public key is published and the private key is kept secret. Data is encrypted with the public key and the same data is decrypted with the corresponding private key. Digital signatures are used when you are encrypting some important information that is to be kept confidential. Digital signatures involve the use of hash tables that encrypt a hash using the private key and decrypt the hash using the private key. Electronic money has surely changed the business and banking techniques. Electronic money has enabled anytime and anywhere banking facility. Due to advent in information technology and IT infrastructural development, Indian banks started offering e-payment in India.

3.2.4 E-payment in India

The vehicle for carrying e-payment is internet. Due to ICT initiative from Indian Government the usage of internet has increased since last 10 years. As shown in figure 3.4, number of internet users reached 81,000,000 in 2010. The Internet Penetration (% Population) was 8.5% is less compared world Internet Penetration of 28.7% as on 2010.
Figure 3.4: Graph showing Internet users in India (1998-2010)

Hence the e-commerce adoption in India is also low as it directly involves internet user’s adoptability to current IT environment due to its slow data transfer and their apprehension about lack of security in data transmission.

India’s share of online commerce is projected to grow from 1.3 percent of Asia-Pacific in 2006 to 3.3 percent by 2011. The projected value of the market is $4.1 billion and $5.6 billion in 2011.

According to IAMAI, a trade association that presents the online content and advertising, e-commerce and mobile content and advertising industry, Indian citizens use Internet for a number of activities including e-mail and IM - 98%, job search – 51%, e-banking – 32%, bill payment -18%, stock trading – 15%, and matrimonial search – 15%. E-banking is catching up in India.

According to RBI report 2010 the payment industry is set to see significant alteration in its value chain with the introduction of online payment. The online payment market which has grown in importance in recent years as a result of boom in the e-commerce market has resulted in the shift of customers from paper based payment mediums to online payment mediums.
The consumer preferences are shifting towards transparency and flexibility as they are looking for better, more proactive solutions around life events. The payment system under retail electronic banking system has steadily increased from 2007-2010 that is evident from Electronic fund transfer under NEFT, as more bank customers opted for online services due adoption of latest ICT. The credit/debit card spending has also increased in the 2007-2010 period. Most of the bank customers used debit card for their financial transactions instead of visiting branch for transactions. This is shown in the table 3.1.

### Table 3.3: Indian banks payment system (Annual turnover) - Retail Electronic Clearing (RBI report 2010)

<table>
<thead>
<tr>
<th></th>
<th>2007-08</th>
<th>2008-09</th>
<th>2009-10</th>
<th>2007-08</th>
<th>2008-09</th>
<th>2009-10</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. ECS DR</td>
<td>1,27,120</td>
<td>1,60,055</td>
<td>1,50,214</td>
<td>48,937</td>
<td>66,976</td>
<td>69,819</td>
</tr>
<tr>
<td>2. ECS CR</td>
<td>78,365</td>
<td>88,394</td>
<td>98,550</td>
<td>7,82,222</td>
<td>97,487</td>
<td>1,17,833</td>
</tr>
<tr>
<td>3. EFT/NEFT</td>
<td>13,315</td>
<td>32,161</td>
<td>66,357</td>
<td>1,40,326</td>
<td>2,51,956</td>
<td>4,11,088</td>
</tr>
<tr>
<td>4. Credit Cards</td>
<td>2,28,208</td>
<td>2,59,561</td>
<td>2,34,209</td>
<td>57,985</td>
<td>65,356</td>
<td>62,950</td>
</tr>
<tr>
<td>5. Debit Cards</td>
<td>88,306</td>
<td>1,27,654</td>
<td>1,70,170</td>
<td>12,521</td>
<td>18,547</td>
<td>26,566</td>
</tr>
<tr>
<td>Total Retail Electronic Clearing Cards</td>
<td>2,18,800</td>
<td>2,80,610</td>
<td>3,15,121</td>
<td>9,71,485</td>
<td>4,16,419</td>
<td>5,98,740</td>
</tr>
</tbody>
</table>

Indian payment industry has witnessed sea change since the introduction of online payment as more and more consumers are shifting from traditional method of making payment i.e. paper based to the new payment methods like online bill payment and card based payment methods. The most preferred payment instrument for online payment in India is credit cards. According to VISA, in 2008, 57% of internet users from India had shopped online, mainly on Airline tickets, Travel accommodation and online travel agents. According to ABC payments, the financial transactions from online
banking in India are expected to outpace credit card transactions in the forthcoming years.

Hence it is advisable to have payment gateways which offer one common platform with one point contact for all banking transactions. The list of very popular payment gateways in India are as follows:

- CCAvenue
- PaisaPay
- Transecute
- ebs.in
- direcpay
- ABC Payments
- HDFC/ICICI/Axis
- Payseal ICICI
- Eazy2Pay
- PayGateIndia
- Epayments.in

The 92 payment gateways are there from other countries who are offering following services (Appendix – I)

3.2.5 Brief review of current e-payment schemes

In general, an e-payment system must exhibit integrity, authorization, confidentiality, and anonymity for security requirements\(^{32}\). Additionally, there are some other important characteristics such as interoperability, scalability, etc. Specific systems are designed to meet specific requirements, and how these characteristics are balanced poses a challenge to future development.

Payment systems can be classified in a variety of ways according to their characteristics such as the exchange model (cash-like, cheque-like or hybrid), central authority contact (online or offline), or hardware requirements (specific or general), etc.
3.2.6 Types of e-payment

Over last 10 years IT adoption steadily increased in banking sector due to customers demand for faster banking transactions. This led to different approach in offering e-payment. These e-payments methods evolved are internet banking, ATM, Tele-Banking, e-cash, e-wallet, credit/debit card and smart card.

3.2.7 Internet banking

Internet banking allows us to handle many banking transactions via personal computer (PC)/mobile/smart phones. For instance, one can use these devices to access account, check balance, request transfers between accounts, and pay bills electronically.

Internet banking system and method in which a personal computer is connected by a network service provider directly to a host computer system of a bank such that customer service requests can be processed automatically without need for intervention by customer service representatives. The system is capable of distinguishing between those customer service requests which are capable of automated fulfillment and those requests which require handling by a customer service representative. The system is integrated with the host computer system of the bank so that the remote banking customer can access other automated services of the bank. The method includes the steps of inputting a customer banking request from among a menu of banking requests at a remote personnel computer; transmitting the banking requests to a host computer over a network; receiving the request at the host computer; identifying the type of customer banking request received; automatic logging of the service request, comparing the received request to a stored table of request types, each of the request types having an attribute to indicate whether the request type is capable of being fulfilled by a customer service representative or by an automated system; and, depending upon the attribute, directing the request either to a queue for handling by a customer service representative or to a queue for processing by an automated system.
3.2.8 Automated teller machines (ATM)

An unattended electronic machine in a public place, connected to a data system and related equipment and activated by a bank customer to obtain cash withdrawals and other banking services. Also called automatic teller machine/cash machine/ money machine.

An automated teller machine or automatic teller machine (ATM) is an electronic computerized telecommunications device that allows a financial institution's customers to directly use a secure method of communication to access their bank accounts, order or make cash withdrawals (or cash advances using a credit card) and check their account balances without the need for a human bank teller. Many ATMs also allow people to deposit cash or cheques, transfer money between their bank accounts, top up their mobile phones' pre-paid accounts or even purchase postage stamps.

On most modern ATMs, the customer identifies him or herself by inserting a plastic card with a magnetic stripe or a plastic smartcard with a chip that contains his or her account number. The customer is allowed to transact by entering a passcode, often referred to as a PIN (Personal Identification Number) of four or more digits. Upon successful entry of the PIN, the customer may perform a transaction.

If the number is entered incorrectly several times in a row (usually three attempts per card insertion), some ATMs will attempt retain the card as a security precaution to prevent an unauthorized user from discovering the PIN by guesswork. Captured cards are often destroyed if the ATM does not belong to the card issuing bank, as non-customer's identities cannot be reliably confirmed. The Indian market has approximately more than 43651 ATM's as on May 2010.

3.2.9 Tele-banking/Phone banking

Undertaking a host of banking related services including financial transactions from the convenience of customers chosen place anywhere across the globe and any time of day/night has now been made possible by introducing on-line Tele banking services. By dialing the given Tele-banking number through a landline or a mobile from anywhere, the customer can access his account and by following the user-friendly menu, entire banking
can be done through Interactive Voice Response (IVR) system. With sufficient numbers of hunting lines made available, customer call will hardly fail. The system is usually bi-lingual and has following facilities offered

- Automatic balance voice out for the default account.
- Balance inquiry and transaction inquiry in all
- Inquiry of all term deposit account
- Statement of account by Fax, e-mail or ordinary mail.
- Cheque book request
- Stop payment which is on-line and instantaneous
- Transfer of funds with CBS which is automatic and instantaneous
- Utility Bill Payments
- Renewal of term deposit which is automatic and instantaneous
- Voice out of last five transactions.

Digital TV Banking- Using the standard digital reception equipment (set top box and remote control); users can access their bank account. Abbey National and HSBC services are available via Digital TV providers. One of its main selling points is that no account details are transmitted via the World Wide Web;

Text Phone Banking - HSBC have introduced this service to allow customers with text phones to check their balance, pay bills and transfer money.

3.2.10 E-cheque

An E-cheque is the electronic version or representation of paper cheque. The information and legal framework on the E-cheque is the same as that of the paper cheque. It can now be used in place of paper cheque to do any and all remote transactions.

An E-cheque work the same way a cheque does, the cheque writer "writes" the E-cheque using one of many types of electronic devices and "gives" the E-cheque to the payee electronically. The payee "deposits" the Electronic Cheque, receives credit, and the payee's bank "clears" the E-
cheque to the paying bank. The paying bank validates the E-cheque and then "charges" the cheque writer's account for the check.

### 3.2.11 E-cash

The twenty-first century, payments by electronic or digital cash, which allow consumers to pay for goods and services by transmitting a code from one computer to another? These code function much like the serial numbers on "real money." They are unique, and represent a specific amount of actual cash.

Unlike credit-card transactions, electronic-cash transactions are anonymous. E-cash works just like paper cash. Once it is withdrawn from an account it does not leave a trail of digital image. E-cash by its nature is portable and therefore more convenient for mobile commerce (mobile internet phones and personal digital assistants (PDA).

Consumers deposit money into a special account or a bank. The bank issues numerals for specific amounts. The money is withdrawn from the consumer's account in the form of a certificate and transferred into the vendor's account for purchases. Like paper money, it can be reused as long as there's money in the bank to back it up. Rather than send a check, a buyer can send electronic cash over the internet in encoded email. This convenience has made electronic pay systems like "Pay Pal" extremely popular with online auction sites where individuals carryout the transactions. A person can even send e-cash to a child at college or to a family member or friend who lives across town or on the other side of the world.

Electronic cash is not always protected in the case of theft or fraud like credit cards. In a recent case, a dealer who knew how to get around the system scammed several Yahoo! auction participants who used Pay Pal.

### 3.2.12 E-wallet

An E-wallet (also known as a digital-wallet) allows users to make electronic commerce transactions quickly and securely.

An E-wallet functions much like a physical wallet. The E-wallet was first conceived as a method of storing various forms of electronic money (e-cash), but with little popularity of such e-cash services, the E-wallet has evolved into
a service that provides internet users with a convenient way to store and use online shopping information.

A client side E-wallet requires minimal setup and is relatively easy to use. The setup requires installation software and the pertinent user information. At the purchase/check-out page of an e-commerce site, the E-wallet software has the ability to automatically enter the user information in the online form. By default, most E-wallets prompt when the software recognizes a form in which it can fill out, if you chose to automatically fill out the form, you will be prompted for a password. This keeps unauthorized users from accessing personal information stored on a particular computer.

3.2.13 Credit card

A credit card is a small plastic card issued to users as a system of payment. 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 grants a line of credit to the consumer (or the user) from which the user can borrow money for payment to a merchant or as a cash advance to the user. Usage of the term "credit card" to imply a credit card account is a metonym.

A credit card is different from a charge card: a charge card requires the balance to be paid in full each month. In contrast, credit cards allow the consumers a continuing balance of debt, subject to interest being charged. Most credit cards are issued by banks or credit unions, and are the shape and size specified by the ISO/IEC 7810 standard as ID-1. This is defined as 85.60 × 53.98 mm (3.370 × 2.125 in) (33/8 × 21/8 in) in size. Figure 3.5 shows a sample credit card.
Credit cards are issued after an account has been approved by the credit provider, after which cardholders can use it to make purchases at merchants accepting that card.

When a purchase is made, the credit card user agrees to pay the card issuer. The cardholder indicates consent to pay by signing a receipt with a record of the card details and indicating the amount to be paid or by entering a personal identification number (PIN). Also, many merchants now accept verbal authorizations via telephone and electronic authorization using the internet, known as a 'Card/Cardholder Not Present' (CNP) transaction.

### 3.2.14 Credit card transaction processing systems

There are two main types of credit card payment processing systems. They are merchant account processing and third party credit card transaction processing. The credit card transaction process is different in both systems.

Merchant account credit card transaction processing is a type of credit card transaction processing where the money is directly processed by the merchant account providing bank.

- Client enters the necessary information using a secure form on the web site.
- This information is encrypted using Secured Socket layer (SSL) encrypted technology
• The encrypted data is passed to the credit card transaction processing gateway
• The data is decrypted using an SSL certificate by the gateway
• The credit card transaction processing gateway verifies the correctness of the information provided. The information is re-encrypted using SSL technology and passed on to the credit card transaction processing bank.
• The bank transfers the money from the clients credit card to merchant account

Third party credit card transaction processing is another type of credit card transaction processing. Here the money is transferred through a third party credit card transaction processing company to the bank. This is used when it is difficult to acquire a merchant account due to the banks’ strict guidelines and credit card transaction processing policies.

• Client enters the necessary information using a secure form on the website
• This information is encrypted using SSL-encryption technology
• The encrypted data is passed to the third party credit card transaction processing company
• The third party credit card transaction processing transfers the data to the banks’ gateway
• The credit card transaction processing gateway verifies the information and passed it to the bank
• The bank transfers the money from the clients credit card to the third merchant credit card transaction processing company
• The third party credit card transaction processing company transfers the money to third party merchant account
• Payouts are then made by bank transfer, cheques, PayPal, etc.

The credit card transaction processing systems have different transaction fees. Third party credit card transaction processing does not have any monthly (or membership) fees, but a higher credit card transaction fee only.
3.2.15 Smart cards

A smart card is a plastic card about the size of a credit card, with an embedded microchip that can be loaded with data, used for telephone calling, electronic cash payments, and other applications, and then periodically refreshed for additional use. A sample smart card is shown in figure 3.6.

Figure 3.6: Smart card

Transactions using smart card are:
- Dial a connection on a mobile telephone and be charged on a per-call basis
- Establish user identity when logging on to an internet access provider or to an online bank
- Pay for parking at parking or to get on subways, trains, or buses
- Provide hospitals or doctors personal data without filling out a form
- For small purchases at electronic stores on the Web

The smart cards are popular in Europe region with over a billion users. Compaq and Hewlett-Packard are reportedly working on keyboards that include smart card slots that can be read like bank credit cards. The hardware for making the cards and the devices that can read them is currently made principally by Bull, Gemplus, and Schlumberger.

A smart card contains more information than a magnetic strip card and it can be programmed for different applications. Some cards can contain
programming and data to support multiple applications and some can be updated to add new applications after they are issued. Smart cards can be designed to be inserted into a slot and read by a special reader or to be read at a distance, such as at a toll booth. Cards can be disposable (as at a trade-show) or reloadable (for most applications).

An industry standard interface between programming and PC hardware in a smart card has been defined by the PC/SC Working Group, representing Microsoft, IBM, Bull, Schlumberger, and other interested companies. Another standard is called OpenCard. There are two leading smart card operating systems: JavaCard and MULTOS.

3.3 E-FRAUDS

3.3.1 Introduction to e-fraud

In India, the banking fraud is not so alarming compared to US and European banking sector, still it poses formidable challenge to Indian banking industry. Its effect can be felt from the fact that in the year 2004 number of cyber crime(IT act 2000 category) were 347 in India which rose to 481 in 2005 showing an increase of 38.5% while I.P.C. category crime stood at 302 in 2005 including 186 cases of cyber fraud and 68 cases cyber forgery. Thus the increasing in frauds in India is matter of concern and such frauds should be dealt with firmly. Otherwise e-banking may become a mere tool in the banking services.

In the present day global scenario, the banking system has acquired new dimensions. The banking system has entered into competitive markets in areas covering resource mobilization, human resource development, customer services and credit management. Due to these ever expanding banking services, the bank frauds have increased in last 5 years.

3.3.2 Frauds in India

In 2009, the Internet fraud has resulted in a loss of ` 6.6 Crores to Indian Banks from 233 reported cases. The number of credit card frauds rose from 2994 case involving ` 532 lakhs to 12959 case involving ` 3654 lakhs in 2008. It is steadily increasing According to Orissa government
statistics, over 13,000 credit card fraud cases were reported in India between April and December 2009. The loss of revenue stood at approximately `36.5 crore in 2008. A loss of `1147 lakhs in such transactions belonged to ICICI Bank which reported over 8280 cases. According to RBI, 2008 report, the number of fraud cases reported was 2658 in 2005, 2568 in 2006 and 2933 in 2007 in public sector banks in India. The table 3.1 shows the number of frauds and amount involved in banks in India from 2004 to 2009.
Table 3.4: Cyber frauds in public/private/foreign banks in India
Number of Fraud Cases and Amount Involved (Including Credit Card Segment) as Reported by Banks to RBI in India
(2005 to 2009)

(Amount: ` in Crore)

<table>
<thead>
<tr>
<th></th>
<th>Number of frauds</th>
<th>Amount Involved</th>
<th>Number of frauds</th>
<th>Amount Involved</th>
<th>Number of frauds</th>
<th>Amount Involved</th>
<th>Number of frauds</th>
<th>Amount Involved</th>
<th>Number of frauds</th>
<th>Amount Involved</th>
</tr>
</thead>
<tbody>
<tr>
<td>2004</td>
<td></td>
<td></td>
<td>2005</td>
<td></td>
<td>2006</td>
<td></td>
<td>2007</td>
<td></td>
<td>2008 – 09</td>
<td></td>
</tr>
<tr>
<td>Public</td>
<td>2193</td>
<td>623.01</td>
<td>2658</td>
<td>1134.39</td>
<td>2568</td>
<td>844.76</td>
<td>2933</td>
<td>793.38</td>
<td>2561</td>
<td>1321.03</td>
</tr>
<tr>
<td>Private</td>
<td>6169</td>
<td>222.23</td>
<td>6169</td>
<td>222.23</td>
<td>14432</td>
<td>322.07</td>
<td>12316</td>
<td>223.71</td>
<td>13241</td>
<td>432.04</td>
</tr>
<tr>
<td>Foreign</td>
<td>3547</td>
<td>29.29</td>
<td>3547</td>
<td>29.29</td>
<td>4687</td>
<td>34.04</td>
<td>7031</td>
<td>60.75</td>
<td>8043</td>
<td>54.23</td>
</tr>
<tr>
<td>Total</td>
<td>11909</td>
<td>874.53</td>
<td>12374</td>
<td>1385.91</td>
<td>21687</td>
<td>1200.87</td>
<td>22280</td>
<td>1077.84</td>
<td>23845</td>
<td>1807.3</td>
</tr>
</tbody>
</table>
India’s banking system has several outstanding achievements to its credit, the most striking of which is its reach. In fact, Indian banks are now spread out into the remotest areas of our country. Indian banking, which was operating in a highly comfortable and protected environment till the beginning of 1990s, has been pushed into the intense competition. A sound banking system should possess three basic characteristics to protect depositor's interest and public faith.

These are:
- Frad free culture,
- Time tested best practice code, and
- In house immediate grievance remedial system

All these conditions are missing or extremely weak in India. Section 5(b) of the Banking Regulation Act, 1949 defines banking as "Banking is the accepting deposits of money for the purpose of lending or investment from the public, repayable on demand or otherwise and withdrawal by cheque, draft, order or otherwise." But if the money has fraudulently been drawn from the bank the latter is under strict obligation to pay the depositor. The bank therefore has to ensure at all times that the money of the depositors is not drawn fraudulently. Time has come when the security aspects of the banks have to be dealt with on priority basis. The banking system in our country has been taking care of all segments of our socio-economic set up.

A bank fraud is a deliberate act of omission or commission by any person carried out in the course of banking transactions or in the books of accounts, resulting in wrongful gain to any person for a temporary period or otherwise, with or without any monetary loss to the bank.

3.3.3 Frauds in U.S.A

In U.S.A, during January 1, 2008 – December 31, 2008, the internet crime complaint center (IC3) website received 275,284 complaint submissions. This is a (33.1%) increase when compared to 2007 when 206,884 complaints were received. These filings were complaints primarily related to fraudulent and non-fraudulent issues on the internet. Figure 3.7
shows the top ten IC3 complaints categories and percent of total complaint received.

![Top 10 Crime type in US](image)

**Figure 3.7: Top ten IC3 complaints categories**

Going by the statistics released in 2009, the Internet Crime Complaint Center (IC3) of the US Federal Bureau of Investigation (FBI) reported losses from internet fraud in 2009 witnessed more than twofold increase over 2008 – from $264.6 million to $559.7 million.

From 2001 to 2007, the FBI sought an increase of more than 1,100 agents for criminal investigations apart from national security. This shows the severity in the financial frauds during 8 years. Credit card fraud is the number one problem in e-commerce. With about 93 percent of all consumer internet purchases made with credit cards, credit card frauds are on the rise. In fact, a Gartner survey of 100 web retailers found Internet credit-card fraud to be much more common than offline fraud, making it the "No. 1 problem" in e-commerce.

Internet frauds that victimize the merchants are becoming shrewder, wiser and more sophisticated. In fact, gone are the days when credit-card
thieves have to break into web servers to steal card numbers. All they have to do is to download software on the internet to generate a supply of credit card numbers associated with a particular bank.

The federal Fair Credit Billing Act limits consumer liability for all incidents of credit card fraud to only $50 of any unauthorized charges. Thus, online merchants often stand to lose the most from online fraud. Beyond the expenses of charge-backs and bank fees (which are higher than those paid by their traditional retail counterparts), companies that gain reputations as vulnerable to online fraud often lose customer confidence and business.

The CSI/FBI Computer Crime and Security Survey\textsuperscript{36} for 2000 indicated that 44 percent of all companies interviewed revealed that they failed to report incidents, while 20 percent notified their legal counsel, and only 25 percent went to law enforcement agencies. More than half stated that they wanted to avoid negative publicity or would prefer to handle the situation themselves.

In 2008, due to credit card fraud the average dollar loss per complaint was $223.00 as compared to $1000.00 computer fraud average dollar loss per complaint. Internet frauds have increased to 33 per cent in 2008 causing $265 million loss to the victims. India takes the fifth position, according to a 2008 internet fraud report. US top the list with 275,284 reports (92.4 percent), followed by Canada with 1.77 percent, Britain (0.95 percent), Australia (0.57 percent) and India 0.36 percent.

Phishing is “the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication”\textsuperscript{37} and the United States is the world leader here according to wordpress.com site\textsuperscript{38} (2006). While phishing is not the only way to commit internet fraud it is rather disturbing to see India at 8 % phishing attack.

The study by software vendor trustees found that each bank was subject to about 832 phishing attacks each year, but only one out of every 2.7 phishing URLs reached their intended targets. The rest were blocked using email-based phishing filters or anti-spam systems or the websites were taken down before they could cause any damage.
This meant that an average of 12.5 out of every million customers from any given bank visited a phishing website on receiving a phishing email every year and 4700 handed over their login information.

Financial institutions are subjected to an average of 16 phishing attacks per week, costing them between $2.4 and $9.4 million in losses each year. Figure 3.8 shows the phishing sites by country of host in 2010.

**Top countries hosting phishing website in 2010**

<table>
<thead>
<tr>
<th>Country</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>United States</td>
<td>62%</td>
</tr>
<tr>
<td>South Korea</td>
<td>6%</td>
</tr>
<tr>
<td>Germany</td>
<td>7%</td>
</tr>
<tr>
<td>Canada</td>
<td>6%</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>6%</td>
</tr>
<tr>
<td>France</td>
<td>4%</td>
</tr>
<tr>
<td>Russia</td>
<td>3%</td>
</tr>
<tr>
<td>China</td>
<td>3%</td>
</tr>
<tr>
<td>Italy</td>
<td>3%</td>
</tr>
<tr>
<td>The Netherlands</td>
<td>3%</td>
</tr>
<tr>
<td>Other countries</td>
<td>3%</td>
</tr>
</tbody>
</table>

**Figure 3.8: Pie diagram of phishing sites by country of host**

Payments industry association Apacs reports that the number of phishing attacks, where e-mails which try to persuade unsuspecting victims to provide confidential bank information and personal details. And money mule advertisements, where fraudsters looking to recruit someone to transfer money from one country to another on their behalf, both continue to rise.

Apacs said the number of phishing websites set up in the first half of 2008 increased by 180% and the number of money mule advertisements rose by 33% over 2007.

According to report from Avira antivirus vendor in 2010, Paypal got into the focus of the phishers’ attempts to steal account information again – three
quarter of all phishing attempts attacked PayPal accounts (75%). Ebay accounts seem to be less attractive; the amount of phishing attacks is down to a quarter (2.76%).

3.3.4 Definition of fraud

Fraud is defined as "any behavior by which one person intends to gain a dishonest advantage over another". In other words, fraud is an act or omission which is intended to cause wrongful gain to one person and wrongful loss to the other, either by way of concealment of facts or otherwise.

Fraud is defined under section 421 of the Indian Penal Code and under section 17 of the Indian Contract Act. Thus essential elements of frauds are:

- There must be a representation and assertion
- It must relate to a fact
- It must be with the knowledge that it is false or without belief in its truth
- It must induce another to act upon the assertion in question or to do or not to do certain act.

3.3.5 Bank frauds: concept and dimensions

Banks are the engines that drive the operations in the financial sector, which is vital for the economy of the country. After Independence, the banks have passed through three stages. With the nationalization of banks in India in 1969, they also have emerged as engines for social change. They have moved from the character based lending to ideology based lending to today competitiveness based lending in the context of India's economic liberalization policies and the process of linking with the global economy.

While the operations of the bank have become increasingly significant banking frauds in banks are also increasing and fraudsters are becoming more and more sophisticated and ingenious. In a bid to keep pace with the changing times, the banking sector has diversified its business manifold. And the old philosophy of class banking has been replaced by mass banking. The challenge in management of social responsibility with economic viability has increased.
The variations in the definitions of e-fraud are attributable to a number of factors such as the differing contexts in which e-fraud has been found to occur: for example, the definition given by the USA Department of Justice (DOJ 2001) is consumer oriented. The perceived importance and role of the Internet / technology is other source of variation. In considering the underlying dimensions, domain and outcome differences as well as the differences in how the involvement of technology in the electronic crime is defined, numerous different definitions result. These variations are accommodated within the broad definition put forward by Graham (2001). Using the Graham’s (2001) definition as a basis, the figure 3.9 provides a diagrammatic representation of the e-fraud as the intersection of E-crime and Fraud.

Figure 3.9: Region of E-fraud

Losses sustained by banks as a result of frauds exceed the losses due to robbery, dacoity, burglary and theft—all put together. Unauthorized credit facilities are extended for illegal gratification such as credit allowed against pledge of goods, hypothecation of goods against bills or against book debts. Common modus operandi are, pledging of spurious goods, projecting as high value goods, hypothecating goods to more than one bank, fraudulent removal of goods with the knowledge and connivance with negligent bank staff, pledging of goods belonging to a third party.
An analysis made of cases brings out broadly the under mentioned four major elements responsible for the commission of frauds in banks.

Active involvement of the staff—both supervisor and clerical either independent of external elements or in connivance with outsiders.

Failure on the part of the bank staff to follow exactly laid down instructions and guidelines.

External elements cause to continue indefinitely frauds on banks by forgeries or manipulations of cheques, drafts and other instruments.

There has been a growing collusion between business, top banks executives, civil servants and politicians in power to defraud the banks, by getting the rules bent, regulations flouted and banking norms thrown to the winds.

The figure 3.10 shows the e-fraud model by Pattama Malakedsuwana and Kenneth J. Stevens.

### 3.3.6 E-fraud model

![Diagram of the E-Fraud model](image)

**Figure 3.10 Revised E-Fraud model.**

**Perpetrator**

The perpetrator or attacker in any e-fraud event will be either ‘internal’ or ‘external’ to the organization. Where the target entity is an individual, then presumably all perpetrators will be external, although this highlights the need to be quite careful when defining what is implied by entity, and hence the use of the term entity, rather than organization. Presumably an entity could be a ‘family’, thus allowing a perpetrator to be considered ‘internal’ where they have a close relationship with the family (or are part of the family) and / or intimately aware of the systems in use by family members.
Mode of Attack

Modes of attack are the ‘mechanism’ used to commit fraud. Two broad types are technical and non-technical modes. Non-technical methods include identity deception (simple case of lying) and social engineering (Alexander 1996). Technical modes of attack are numerous and contribute towards the ‘e’ portion of the term. At times, closely related to the target system. Examples of modes of attack include data modification in systems, IP spoofing and use of malicious code. Special attention should be paid to identity fraud, as it may be either technical or non-technical.

Target System

The target system element represents the system through which the fraud will be perpetrated. The target system includes a number of inter-connected systems, some of which may not be owned or controlled by the target entity. Systems that are wholly contained within the entity will presumably be attacked by a different type of perpetrator, using different modes of attack than those that would be used against inter-organizational systems (IOS) that are only partially controlled by the organizations. The inclusion of IOS and e-business systems must improve the prospects of a better understanding of the risk exposure that the systems on which entities rely represent.

Target Entity

The separation of the target entity from the target system allows the characteristics of the entity’s context to be considered without the compounding influence of the systems and distinguishes weaknesses of the technology from the entity characteristics. Entities can be divided into two classes: individuals and organizations. These class share many features (such as lack of awareness) but organizational features such as the existence control systems such as corporate governance, teams of fraud specialists, as well as prevention and detection procedures suggest that these two target groups need to be considered separately.
Impact

Impact is the result of an e-fraud incident, and may include either financial losses or nonfinancial losses. Financial losses include the cost of rectifying the situation (such as consultants coming in to fix the security holes) or actual losses from assets stolen or damaged. Non-financial losses include loss of reputation, loss of competitive advantage and personal distress and loss of wellbeing. Impact is considered separately from target entity as a single incident of e-fraud may have a broad impact across more than just the target entity or entities. This distinction accommodates for any flow on affects where the impact can be an interim result of another ‘crime’ such as identity theft.

Implications of the E-fraud Model

E-fraud needs to be well understood to in order to properly quantify and mitigate the risk exposure. There is a need to see dimensions, the breath and depth of e-fraud. The model presented should assist practitioners to gain a wider view of how organizations and individuals can be affected by e-fraud.

A key point that arises out of the study of dimensions of e-fraud was the prevalence of discussion of identity-related frauds implicitly and explicitly. Firstly, much of the literature identified identity fraud as a category of e-fraud or e-crime explicitly. In many cases identity related crimes were implicit in nature, for example, many white-collar crimes were committed through the use of ‘borrowed’ or stolen identities and passwords (DOJ 2001a, Graycar & Smith 2002). It would seem that identity fraud and e-fraud are intimately linked.

Another implication for the e-fraud model is that in the future this model may help facilitate a better collection of more detailed data and by using a richer data set across the various dimensions identified in the model.

3.3.7 Types of fraud

- Electronic Fraud
- Identity Fraud
• Spy ware and Ad ware
• Debit/Credit Card Fraud

3.3.8 Electronic fraud

This refers to email scams from fraudsters to obtain banking and personal information and here is how it works: The person receives an email appearing to be from NBK Company or another legitimate company in or out of a country.

The email may claim a number of different things such as:

- There is a problem with your account
- Ask you to enter a contest to win a prize
- Ask you to subscribe to a service that will provide you with prizes and etc.
- You are then asked to provide your personal and financial information by completing an online form.

The form requests a variety of information such as:

- Your credit card numbers
- Your account number
- Your passport or Civil ID numbers and so forth

Once you provide this information the fraudsters will have the necessary information on you to conduct a fraud. Here is an example of an email fraud as shown in figure 3.11
Numerous definitions of e-fraud have been advanced in the e-crimes literature. Graham (2001) defines e-fraud as “a fraudulent behavior connected with computerization by which someone intends to gain dishonest advantage”. In this definition e-fraud equates to, and supersedes, the term computer fraud. Some definitions specify e-fraud in relation to electronic commerce or the Internet such as Smith (2001) in which e-fraud is seen as “any dishonest activity that involves the Internet as the target or means of obtaining some financial reward”. The USA Department of Justice also defines e-fraud in relation to the Internet.

“A fraud scheme that uses one or more components of the Internet - such as chat rooms, e-mail, message boards, or web sites - to present fraudulent solicitations to prospective victims, to conduct fraudulent transactions, or to transmit the proceeds of fraud to financial institutions or to other connected with the scheme”.39

Alternatively, some studies40 define such crimes as ‘Internet fraud’,

3.3.9 Identity fraud

Identity fraud is where a dishonest person will gather personal details in order to conduct a fraud which will financially hurt the user. These fraudsters can obtain user personal information in a number of ways, via telephone scams or on the internet.
The following can be used to assume customer identity:

- Date of birth
- Address
- Personal ID number or other identification numbers
- Mobile phone number
- Banking information

### 3.3.10 Spyware and Adware

Spyware is a type of software that secretly collects user personal and information while on the Internet.

Adware is a type of spyware used to track visitors' habits and interests on the Internet. Adware can monitor the types of sites user visit, the articles read or the type's banners user click on and so forth. Many times this information is sold to a third party for the purpose of marketing.

### 3.3.11 Wire fraud

Wire transfer networks such as the international, interbank fund transfer system are tempting as targets as a transfer, once made, is difficult or impossible to reverse. As these networks are used by banks to settle accounts with each other, rapid or overnight wire transfer of large amounts of money are commonplace; while banks have put checks and balances in place, there is the risk that insiders may attempt to use fraudulent or forged documents which claim to request a bank depositor's money be wired to another bank, often an offshore account in some distant foreign country.

### 3.3.12 Theft of identity

Dishonest bank personnel have been known to disclose depositors' personal information for use in theft of identity frauds. The perpetrators then use the information to obtain identity cards and credit cards using the victim's name and personal information.
3.3.13 Credit card fraud

Credit card and debit card fraud is a crime where credit or debit cards are reproduced by criminals. This type of crime is known as 'skimming'.

Credit or debit card fraud can also occur when user card is lost or stolen and used by fraudster to purchase goods or remove cash from ATMs or other locations.

Credit card fraud is a multi-billion-currency a year loss for banks and the government. With the progression of computers and e-commerce, hackers are able to exploit more information more easily without ever having to leave their homes. Now, entire departments of organizations in the criminal justice system are being dedicated to preventing and finding cyber-crimes.

There are many ways that scammers can actually get user information. This can be as simple as mass sending an e-mail impersonating a bank and linking to a look-alike website luring you to enter your financial information there, or they can be as complicated as stealing information off the real bank website through complicated computer viruses. Financial institution look-alike websites can be found all over the internet, and can be very convincing. This method generally isn’t very involved, as it is quite easy to design or find a website that remotely looks like bank institutions. This method has also been around the longest and has motivated financial websites to secure their websites more. The look-alike websites are coded to look and act likes the normal website, with one difference: The information submitted to the site goes to the hacker’s databases rather than the banks.

Another method of obtaining financial information is ATM skimming. Popular recently, this method involves putting a mechanism on the ATM’s card slot that reads that magnetic strip. If placed correctly, these machines can be very effective, because the user still is able to go through with their transaction on the ATM. The device has a small magnetic reader called an MSR, and a small memory card that records all cards inserted. Magnetic strips have two important strings of information on them, called Track 1 and Track 2. Although only one is needed for a bank transaction, both tracks are usually paired and exploited together. The more informative Track 1 contains account number, expiration date, card verification value (CVV2) code, and name of account holder. This, of course, is all the information needed to steal
money from the account holder. The data dumped from the memory cards, are called “dumps”.

Knowing store owners or other knowledgeable people, these dumps can be exploited. In most cases, dumps are sold without PIN numbers, and only depending on the bank, only $500 can be stolen from the account. However, with a PIN number, the account could be completely emptied at the disposal of the hacker. Of course, greater payouts mean greater effort and risk involved. Retrieving PIN numbers is more involved and requires more advanced technology to retrieve. Dumps are the most complicated form of stolen financial information to cash out, as they require access to a bank wire that only retailers would have. This gets into money laundering and other ways to put on the facade that the money is being earned legitimately.

There is another method that involves using a money transfer service from legitimate money Transfer Company to transfer the money from the stolen account to a separate account. The obstacle hackers have to overcome is the fact that legitimate company operators check the identity of the bank account to the person executing the transaction. This can be overcome by knowing operators or possibly working with them. Operators that are involved with illegal sending of money are known as “drops”, and share the profit with the hacker.

Finally, a more efficient and brute-force method is to steal online retailers’ customer databases. Obviously, this is a gold mine of information for a hacker. In some cases, little effort is required to hack into insecure databases from smaller retailers and can result in massive payouts for the hacker with little effort. The data collected from this method usually can sell on the black market for a higher price, as the data is almost guaranteed to be accurate, and depending on the vendor, quality data can be sold for a varying price on the black market.

In most cases, the hackers that exploit this financial information do not use it directly for financial gain. Instead, they sell the information. Hackers sell three basic things: “dumps” (track 1 and track 2 off the magnetic strips), “CVVs” (all information needed to buy something online), and “fullz” (a cvv plus social security number, mother’s maiden name, date of birth, and PIN number). “CVVs” are usually the cheapest, ranging from $1.50 to $5 a piece,
depending on the age of the information and the type of card (VISA, Mastercard, American Express, Discover). “Fullz” usually sell for $8-$15 dollars, and finally “dumps” can sell for up to $100 depending on the seller. Like anything, discounts are given for buying in greater quantities.

One may be wondering how these exchanges are made. It has been described that the illegal credit card market is like the illegal drug market. The system works in a hierarchical way, prices vary, and there are scammers. Obviously, hackers can use the streets to sell ill-gotten information, through a chat-system called Internet Relay Chat, IRC. IRC is an extremely simple protocol of chat that has been around since the time the internet was invented, and by nature is extremely hard to monitor and track. The only time during which third parties such as the police can monitor chats through IRC, are when the actual exchange is occurring. After the exchange, there is absolutely no record of the chat. There are IRC servers entirely dedicated to illegal credit card distribution, though contain no evidence to prosecute with. Also, every user usually is behind what is called a proxy. A proxy is a server that the user connects to and then uses to connect to the illegal server to avoid being traced. Properly run proxies are extremely hard to trace to the origin, and offer an extra layer of protection. Once connected to the server, users join what are called channels and find literally advertisements from vendors. Buyers find sellers, send them a message, and the exchange is executed. Other forms of communication are personal instant messengers such as Yahoo Messenger and regular e-mail.

Of course, hackers simply can’t pay for the illegal data with conventional methods of internet payment. Hackers commonly use services such as EGOLD, Liberty Reserve, and other forms of electronic metal. E-metal accounts are bank accounts that are 100% backed by gold, silver, platinum, and other precious metals, and they are 100% untraceable and anonymous. Payments are made from one e-metal account to another, and nothing can be traced. Other forms of payment can include services such as Western Union and MoneyGram, and are used for larger purchases usually.
3.3.14 Booster cheques

A booster cheque is a fraudulent or bad cheque used to make a payment to a credit card account in order to "bust out" or raise the amount of available credit on otherwise-legitimate credit cards. The amount of the cheque is credited to the card account by the bank as soon as the payment is made, even though the cheque has not yet cleared. Before the bad cheque is discovered, the perpetrator goes on a spending spree or obtains cash advances until the newly-"raised" available limit on the card is reached. The original cheque then bounces, but by then it is already too late.

3.3.15 Stolen payment cards

Often, the first indication that a victim's wallet has been stolen is a 'phone call from a credit card issuer asking if the person has gone on a spending spree; the simplest form of this theft involves stealing the card itself and charging a number of high-ticket items to it in the first few minutes or hours before it is reported as stolen.

A variant of this is to copy just the credit card numbers (instead of drawing attention by stealing the card itself in order to use the numbers in online frauds.

3.3.16 Duplication or skimming of card information

This takes a number of forms, ranging from a dishonest merchant copying clients' credit card numbers for later misuse (or a thief using carbon copies from old mechanical card imprint machines to steal the info) to the use of tampered credit or debit card readers to copy the magnetic stripe from a payment card while a hidden camera captures the numbers on the face of the card.

Some thieves have clandestinely added equipment to publicly accessible automatic teller machines; a fraudulent card stripe reader would capture the contents of the magnetic stripe while a hidden camera would sneak a peek at the user’s PIN. The fraudulent equipment would then be removed and the data used to produce duplicate cards that could then be used to make ATM withdrawals from the victims' accounts.
3.3.17 Impersonation and theft of identity

Theft of identity has become an increasing problem; the scam operates by obtaining information about a victim, then using the information to apply for identity cards, accounts and credit in that person's name. Often little more than name, parents' name, date and place of birth are sufficient to obtain a birth certificate; each document obtained then is used as identification in order to obtain more identity documents. Government-issued standard identification numbers such as PAN numbers are also valuable to the identity thief.

Unfortunately for the banks, identity thieves have been known to take out loans and disappear with the cash, quite content to see the wrong persons blamed when the debts go bad.

3.3.18 Money laundering

The term "money laundering" dates back to the days of Al Capone. Money laundering has since been used to describe any scheme by which the true origin of funds is hidden or concealed. The operations work in various forms. One variant involved buying securities (stocks and bonds) for cash; the securities were then placed for safe deposit in one bank and a claim on those assets used as collateral for a loan at another bank. The borrower would then default on the loan. The securities, however, would still be worth their full amount. The transaction served only to disguise the original source of the funds. The Finance ministers of G-20, including India has decided to take counter measures against tax heavens particularly non-cooperative ones, to prevent money laundering and terror financing through cyber crimes from 2010.

3.3.19 Difficulties in tracking bank frauds

Hi-tech crime

The information technology is changing very fast. The normal investigator does not have the proper background and knowledge. Special investigators have to be created to carry out the investigations. The FBI of USA have a cell, even in latest scenario there has been cells operating in the Karnataka/ Maharashtra/Punjab police departments to counter cyber crimes. CBI also has created special team for fighting cyber crimes.
International crime

A computer crime may be committed in one country and the result can be in another country. There has been a lot of jurisdictional problem although the Interpol does help but it too has certain limitations. The different treaties and conventions have created obstructions in relation to tracking of cyber criminals hiding or operation in other nations.

No-scene crime

The computer satellite computer link can be placed or located anywhere. The usual crime scene is the cyber space. The terminal may be anywhere and the criminal need not indicate the place. The only evidence a criminal leaves behind is the loss to the crime.

Faceless crime

The major advantage criminal has in instituting a computer crime is that there is no personal exposure, no written documents, no signatures, no fingerprints or voice recognition. The criminal is truly and in strict sense faceless. There are certain spy software's which is utilized to find out passwords and other vital entry information to a computer system. The entry is gained through a spam or bulk mail. The Reserve Bank of India has come up with different proposals to make the way easier; they have enacted electronic fund transfer act and regulations from time to time.

The enacted laws of India from 2000 to till now are not at all adequate to counter cyber crimes. In the past nine years, 307 cases have been registered in Bangalore's specially set up cyber crime police station. Of them 80 per cent relate to hacking and misuse of bank accounts. The police have filed charge sheets in 60 cases. So far no one has been convicted. The Indian Penal code, evidence act, and criminal procedure code had no clue about computers when they were codified. It is highly required to frame and enact laws which would deal with those subjects which are new to the country specially cyber law; Intellectual property right etc. Though IT act 2000 was the first step towards combating cyber crimes and encouraged e-commerce in India, the act was not implemented properly. Hence IT Act 2000 was again revised in 2010 with more stringent laws to counter ever increasing cyber frauds in India.