CHAPTER - 2

Internet Banking : A new paradigm shift

☑ Internet : Basic Structure and Topology

☑ Internet Banking: International Experience

☑ Internet Banking: The Indian Scenario

☑ Internet Banking and its various types

☑ Risks associated with Internet banking

CHAPTER : 2

INTERNET BANKING : A NEW PARADIGM SHIFT

2.1 Internet : Basic Structure and Topology :

Internet is a vast network of individual computers and computer networks connected to and communicate with each other using the same communication protocol – TCP/IP (Transmission Control Protocol / Internet Protocol). When two or more computers are connected a network is created; connecting two or more networks create 'internet work' or Internet. The Internet, as commonly understood, is the largest example of such a system. Internet is often and aptly described as 'Information Superhighway', a means to reach innumerable potential destinations. The destination can be any one of the connected networks and host computers. Internet has evolved to its present state out of a US Department of Defence project ARPA Net (Advanced Research Project Administration Network), developed in the late 1960s and early 1970s as an experiment in wide area networking. A major perceived advantage of ARPA Net was that the network would continue to operate even if a segment of it is lost or destroyed since its operation did not depend on operation of any single computer [1].

Though originally designed as a defence network, over the years it was used predominantly in areas of scientific research and communication. By the 1980s, it moved out of Pentagon's control and more independent networks from US and outside got connected to it. In 1986, the US National Science Foundation (NSF) established a national network based on ARPA protocol using commercial telephone lines for connectivity. The NSF Net was accessible by a much larger scientific community, commercial networks and general users and the number of host computers grew rapidly. Eventually, NSF Net became the framework of today's Internet. ARPA Net was officially decommissioned in 1990.

It has become possible for innumerable computers operating on different platforms to communicate with each other over Internet because they adopt the same communication protocol, viz, TCP/IP. The latter, which stands for 'Transmission Control Protocol / Internet Protocol', is a set of rules which define how computers communicate with each other. In order to access Internet one must have an account in a host computer, set up by any one of the ISPs (Internet Service Providers). The accounts can be SLIP (Serial Line Internet Protocol) or PPP (Point to Point Protocol) account. These accounts allow creating temporary TCP/IP sessions with the host, thereby allowing the computer to join the Internet and directly establish communication with any other computer in the Internet. Through this type of connection, the client computer does not merely act as a remote terminal of the host, but can run whatever programs are available on the web. It can also run several programs simultaneously, subject to limitations of speed and memory of the client computer and modem. TCP/IP protocol uses a unique addressing scheme through which each computer on the network is identified.

TCP / IP protocol is insecure because data packets flowing through TCP / IP networks are not normally encrypted. Thus, any one who interrupts communication between two machines will have a clear view of the data, passwords and the like. This has been addressed through Secured Socket Layer (SSL), a Transport Layer Security (TLS) system which involves an encrypted session between the client browser and the web server.

FTP or File Transfer Protocol is a mechanism for transferring files between computers on the Internet. It is possible to transfer a file to and from a computer (ftp site) without having an account in that machine. Any organization intending to make available to public its documents would normally set up a ftp site from which any one can access the documents for download. Certain ftp sites are available to validated users with an account ID and password. [2]

E-mail:

The most common and basic use of Internet is the exchange of e-mail (electronic mail). It is an extremely powerful and revolutionary result of Internet, which has facilitated almost instantaneous communication with people in any part of the globe. With enhancements like attachment of documents, audio, video and voice mail, this segment of Internet is fast expanding as the most used communication medium for the whole world. Many websites offer e-mail as a free facility to individuals. Many corporate have interfaced their private networks with Internet in order to make their email accessible from outside their corporate network

World Wide Web (WWW):

Internet encompasses any electronic communication between computers using TCP/IP protocol, such as e-mail, file transfers etc. WWW is a segment of Internet, which uses Hyper Text Markup Language (HTML) to link together files containing text, rich text, sound, graphics, video etc. and offers a very convenient means of navigating through the net. It uses hypertext transfer protocol (HTTP) for communication between computers. Web documents, which are referred to as pages, can contain links to other related documents and so on, in a tree like structure. The person browsing one document can access any other linked page. The web documents and the web browsers which are the application programs to access them are designed to be platform independent. [3]

Thus any web document can be accessed irrespective of the platform of the computer accessing the document and that of the host computer. The programming capabilities and platform independence of Java and Java applets have further enriched the web. The 'point and click' method of browsing is extremely simple for any lay user of the net. In fact, the introduction of web since early 1990 has made Internet an extremely popular medium and its use in business has been enhanced dramatically. The next in the HTML genre is the Extensible Markup Language (XML), which allows automated two-way information flow between data stores and browser screens. XML documents provide both the raw content of data and the data structure and is projected by its proponents as taking the web technology beyond the limits of HTML. [4]

Wireless Application Protocol (WAP):

WAP is the latest industry standard which provides wireless access to Internet through handheld devices like a cellular telephone. This is an open standard promoted by WAP forum and has been adopted by world's all major handset manufacturers. WAP is supplemented by Wireless Application Environment (WAE), which provides industry wise standard for developing applications and services for wireless communication networks. This is based on WWW technology and provides for application for small screens, with interactive capabilities and adequate security.[5] Wireless Transaction Protocol (WTP), which is the equivalent of TCP, sets the communication rules and Wireless Transport Layer Security (WTLS) provides the required security by encrypting all the session data. WAP is set to revolutionize the commercial use of net.

Security:

One of the biggest attractions of Internet as an electronic medium is its openness and freedom. It is a public domain and there is no restriction on who can use it as long as one adheres to its technical parameters. This has also given rise to concerns over the security of data and information transfer and privacy. These concerns are common to any network including closed user group networks. But over the Internet, the dimensions of risk are larger while the control measures are relatively fewer. It will be sufficient to say here that the key components of such concern are, (i) authentication, viz., assurance of identity of the person in a deal, (ii) authorization, viz., a party doing a transaction is authorized to do so, (iii) the privacy or confidentiality of data, information relating to any deal, (iv) data integrity, viz., assurance that the data has not been altered and (v) non repudiation, viz., a party to the deal can not deny that it originated the communication or data.[6]

2.1.1 E-Commerce:

Even though started as network primarily for use by researchers in defence and scientific community, with the introduction of WWW in early 1990s, use of Internet for commerce has grown tremendously. E-commerce involves individuals and business organizations exchanging business information and instructions over electronic media using computers, telephones and other telecommunication equipments. Such form of doing business has been in existence ever since electronic mode of data / information exchange was developed, but its scope was limited only as a medium of exchange of information between entities with a pre-established contractual relationship. However, Internet has changed the approach to e-commerce; it is no longer the same business with an additional channel for information exchange, but one with new strategy and models.

A business model generally focuses on (i) where the business operates, that is, the market, the competitors and the customers, (ii) what it sells, that is, its products and services (iii) the channels of distribution, that is, the medium for sale and distribution of its products and (iv) the sources of revenue and expenditure and how these are affected. Internet has influenced all the four components of business model and thus has come to influence the business strategy in a profound way. The size of the market has grown enormously as technically, one can access the products and services from any part of the world. So does the potential competition. The methods of reaching out to customers, receiving the response and offering services have a new, simpler and efficient alternative, now, that is, Internet. The cost of advertisement, offer and delivery of services through Internet has reduced considerably, forcing most companies to rework their strategies to remain in competition. [7]

A research note by Paul Timmers of European commission had identified eleven business models, which have been commercially implemented. These are e-shop, eprocurement, e-auction, e-mall, Third-party market place, Virtual communities, Value chain service providers, Value chain integrators, Collaboration platforms and Information brokers. He classified business models along two dimensions, i.e, degree of innovation and extent of integration of functions. The innovation ranged from the electronic version of a traditional way of doing business (e-shop) to more innovative ways by offering functions that did not exist before. The second dimension, i.e, extent of integration ranges from a single function business model (like e-shop) to fully integrated functionality (value chain integrator). In the top end of the graph are models, which cannot be implemented in a traditional way and are critically dependent upon information technology and creating value from information flow. Business models, in between these two limits are a combination of both dimensions in different degrees and have some degree of analogy in traditional firms. [8]

2.1.2 Types of E-Commerce:

There are two types of e-commerce ventures in operation: the old brick and mortar companies, who have adopted electronic medium, particularly Internet, to enhance their existing products and services, and / or to offer new products and services and the pure e-ventures who have no visible physical presence. This difference has wider ramifications than mere visibility when it comes to issues like customer's trust, brand equity, ability to service the customers, adopting new business culture and cost. These aspects of e-commerce will be touched upon in the following discussions.

Another way of classifying the e-commerce is by the targeted counterpart of a business, viz, whether the counterpart is a final consumer or another business in the distribution chain. Accordingly, the two broad categories are: Business-to-Consumer (B2C) and Business-to-Business (B2B).

2.1.3 Business-to-Consumers (B2C): [9]

In the B2C category are included single e-shops, shopping malls, e-broking, e-auction, e-banking, service providers like travel related services, financial services etc., education, entertainment and any other form of business targeted at the final consumer. Some of the features, opportunities and concerns common to this category of business irrespective of the business segment, are the following.

Opportunities:

Internet provides an ever-growing market both in terms of number of potential customers and geographical reach. Technological development has made access to Internet both cheaper and faster. More and more people across the globe are accessing the net either through PCs or other devices. The purchasing power and need for quality service of this segment of consumers are considerable. Anybody accessing Internet is a potential customer irrespective of his or her location. Thus, any business targeting final consumers cannot ignore the business potential of Internet.

Internet offers a unique opportunity to register business presence in a global market. Its effectiveness in disseminating information about one's business at a relatively cost effective manner is tremendous. Time sensitive information can be updated faster than any other media. A properly designed website can convey a more accurate and focused image of a product or service than any other media. Use of multimedia capabilities, i.e., sound, picture, movies etc., has made Internet as an ideal medium for information dissemination. However, help of other media is necessary to draw the potential customers to the web site.

The quality of service is a key feature of any e-commerce venture. The ability to sell one's product at anytime and anywhere to the satisfaction of customers is essential for e-business to succeed. Internet offers such opportunity, since the business presence is not restricted by time zone and geographical limitations. Replying to customers' queries through e-mail, setting up (Frequently Asked Questions) FAQ pages for anticipated queries, offering interactive help line, accepting customers' complaints online 24 hours a day and attending to the same, etc. are some of the features of e-business which enhance the quality of service to the customers. It is of crucial importance for an e-venture to realize that just as it is easier to approach a customer through Internet; it is equally easy to lose him. The customer has the same facility to move over to another site.

Cost is an important issue in an e-venture. It is generally accepted that the cost of overhead, servicing and distribution, etc. through Internet is less compared to the traditional way of doing business. Although the magnitude of difference varies depending on the type of business and the estimates made, but there is unanimity that Internet provides a substantial cost advantage and this, in fact, is one of the major driving forces for more number of traditional business adapting to e-commerce and pure e-commerce firms to sprout.

Cost of communication through WWW is the least compared to any other medium. Many a time one's presence in the web may bring in international enquiries, which the business might not have targeted. The business should have proper plans to address such opportunities.

Concerns:

There are a number of obstacles, which an e-commerce venture needs to overcome: Trust of customers in a web venture is an important concern. Many customers hesitate to deal with a web venture as they are not sure of the type of products and services they will receive. This is particularly true in a B2C venture like e-shop, e-mall or e-auction site. Traditional business with well established brands and goodwill and having a physical presence face less resistance from customers in this regard than a pure e-venture.

Many B2C ventures have ultimately to deliver a product or service in physical form to the customer for a deal contracted through Internet. This needs proper logistics, an efficient distribution network, and control over quality of product or service delivered. These issues are not technology related and any let off in this area can drive the customer away to the competitor or from e-commerce.

The privacy of information on the customer's preferences, credit card and bank account details etc. and customers' faith in a system where such privacy is stated to be ensured are important issues to be addressed. These are mainly technological issues, but human factor is important both at the business and at the customers' end and also in building the trust in the system.

Security of a transaction, authenticity of a deal, identification of a customer etc. are important technological and systems issues, which are major sources of concern to ecommerce. Equally important are questions of repudiation of a deal, applicability of law, jurisdiction of tax laws etc. These are important to all forms of e-commerce, whether B2C or B2B and all segments of business, i.e., manufacturing, services and finance and are addressed in different chapters of this report.

Accessibility to Internet by the consumers is an important issue in B2C domain. This is particularly so in countries like India where penetration of PCs and other devices to households for access to Internet is minimal. Also important are availability of bandwidth and other infrastructure for faster and easier access. Considering that e-commerce aims at global market, deficiencies of these kinds in the developing world are no longer concerns confined to these areas, but are global e-commerce concerns.

2.1.4 Business to Business (B2B): [10]

As opposed to B2C e-commerce, in B2B domain, the parties to a deal are at different points of the product supply chain. Typically, in a B2B type domain, a company, its suppliers, dealers and bankers to all the parties are networked to finalize and settle all aspects of a deal, online. Perhaps, only the goods in different stages of processing physically move from the supplier to the dealer. This scenario can be extended to include the shipper, providers of different ancillary services, IT service provider and the payment system gateway, etc., depending on the degree of sophistication of the available systems. Another important feature of a B2B domain, as distinct from B2C, is that business information / data is integrated to the back office systems of parties to a deal and the state of straight through processing (STP) or near STP is achieved. This is a very significant aspect of B2B model of e-commerce, which results in improved profits through lowering cost and reducing inventories.

For example, in a B2B environment, typically, the back office system of a company controls inventory requirement with reference to the order book position updated regularly on the basis of orders received from dealers through Internet. At the optimum level of inventory it raises a purchase order with the supplier, whose system in turn, processes the order and confirms supply. Buyer company's system issues debit instructions on its bank account for payment to the supplier. The buyer's bank credits seller's bank with the cost of sale though a payment gateway or through RTGS system.

Similar series of transaction processes are also initiated between the company and its dealers and their respective banks. Once e-commerce relationship is established between the firms, the transactions of the type shown above can be processed with minimal human intervention and on 24 hours a day and 7 day a week basis. New business models are emerging in B2B domain. There are portals which offer a meeting ground to buyers and sellers of different products in supply chain, more like a buyer-seller meet - in international business. This has enabled relatively smaller companies to enter the global market. Banks in the portal offer financial services for deals settled through the portal.

Technology and networking are important constituents of a B2B type of business domain. Earlier, only large firms could have access to such technology and they used private networks with interface to each other for information flow and transaction processing. A major concern used to be compatibility of EDI platforms across different B2B partners. Internet with WWW and other standard technology have offered opportunity to relatively smaller and medium sized firms to integrate their operations in B2B model and take advantage of the benefits it offers. It has also led to standardization of software platforms.

Other new forms of business models in B2B domain are Application Service Providers (ASP) and Service Integrators. ASPs offer application software online to ecommerce companies who pay for the same according to the use without owning it. Often entire back office processing is taken care of by ASPs and other service integrators. However, the utility of such service providers will to a large extent depend on the business strategy of the e-venture.

The concerns of B2B e-commerce are similar to those of B2C, discussed earlier. The security issues are more pronounced because of high value transfers taking place through the net. So also are the issues relating to privacy of information, law, tax repudiation etc. The other issues of importance to a B2B firm are the choice of appropriate technology, the issue of build or out source, maintenance and training of personnel, etc., since they involve large investments and are critical to success.

Several studies have attempted to assess the relative importance of B2B and B2C business domains. There is wide difference in estimates of volume of business transacted over Internet and its components under B2C and B2B. However, most studies agree that volume of transactions in B2B domain far exceeds that in B2C. This is expected result. There is also a growing opinion that the future of e-business lies in B2B domain, as compared to B2C. This has several reasons some of which are already discussed earlier, like low penetration of PCs to households, low bandwidth availability etc., in a large part of the world. The success of B2C ventures depends to a large extent on the shopping habits of people in different parts of the world. A survey sponsored jointly by Confederation of Indian Industries and Infrastructure Leasing and Financial Services on e-commerce in India in 1999 made the following observations. 62% of PC owners and 75% of PC non-owners but who have access to Internet would not buy through the net, as they were not sure of the product offered.

The same study estimated the size of B2B business in India by the year 2001 to be varying between Rs. 250 billion to Rs. 500 billion. In a recent study done by Arthur Anderson, it has been estimated that 84% of total e-business revenue is generated from B2B segment and the growth prospects in this segment are substantial. It has estimated the revenues to be anywhere between US $ 2.7 trillion to over US $ 7 trillion within the next three years (2003). [11]

2.1.5 The Growth of Internet Banking and common products: [12]

Internet Banking is a product of e-commerce in the field of banking and financial services. In what can be described as B2C domain for banking industry, Internet Banking offers different online services like balance enquiry, requests for cheque books, recording stop-payment instructions, balance transfer instructions, account opening and other forms of traditional banking services.

Mostly, these are traditional services offered through Internet as a new delivery channel. Banks are also offering payment services on-behalf of their customers who shop in different e-shops, e-malls etc. Further, different banks have different levels of such services offered, starting from level-1 where only information is disseminated through Internet to level-3 where online transactions are put through.

Considering the volume of business e-commerce, particularly in B2B domain, has been generating, it is natural that banking would position itself in an intermediary role in settling the transactions and offering other trade related services. This is true both in respect of B2C and B2B domains. Besides, the traditional role of financial intermediary and settlement agents, banks have also exploited new opportunities offered by Internet in the fields of integrated service providers, payment gateway services, etc. However, the process is still evolving and banks are repositioning themselves based on new emerging e-commerce business models.

In B2B scenario, a new form of e-commerce market place is emerging where various players in the production and distribution chain are positioning themselves and are achieving a kind of integration in business information flow and processing (STP or near STP) leading to efficiencies in the entire supply chain and across industries. Banks are positioning themselves in such a market in order to be a part of the financial settlements arising out of transactions of this market and providing wholesale financial services. This needs integration of business information flow not only across the players in the supply chain, but with the banks as well.

With the integration of business information flow and higher degree of transparency, the banks and other financial services institutions have lost some of the information advantage they used to enjoy and factor in to pricing of their products. However, such institutions have the advantage of long standing relationships, goodwill and brand, which are important sources of assurance in a virtual market. [13]

Banks are in fact, converting this goodwill into a business component in e-commerce scenario in providing settlement and other financial services. Some banks have also moved to providing digital certificates for transactions through e-markets. Banks' strategies in B2B market are responses to different business models emerging in e-commerce.

A recent study by Arthur Andersen shows that banks and financial service institutions generally adopt one of three business models to respond to e-business challenges. In the first place, they treat it as an extension of existing business without any significant changes other than procedural and what technology demands. The second strategy takes the same approach as the first but introduces structural changes to the underlying business. In the third approach banks launch e-business platform as a different business from the existing core business and as a different brand of product.

There is no definite answer as to which approach is appropriate. Perhaps it depends on the type of market the bank is operating, its existing competencies and the legal and regulatory environment. It is, however, sure that e-banking is evolving beyond the traditional limits of banking and many new products / services are likely to emerge as ecommerce matures. [14]

2.2 Internet Banking: International Experience: [15]

Internet banking has presented regulators and supervisors worldwide with new challenges. The Internet, by its very nature, reaches across borders and is, for this reason, engaging the attention of regulatory and supervisory authorities all over the world. The experience of various countries, as far as Internet banking is concerned, is outlined in this chapter. [16]

2.2.1 United State of America [USA]: [17]

In the USA, the number of thrift institutions and commercial banks with transactional web-sites is 1275 or 12% of all banks and thrifts. Approximately 78% of all commercial banks with more than $5 billion in assets, 43% of banks with $500 million to $5 billion in assets, and 10% of banks under $ 500 million in assets have transactional web-sites. Of the 1275-thrifts/commercial banks offering transactional Internet banking, 7 could be considered 'virtual banks'. 10 traditional banks have established Internet branches or divisions that operate under a unique brand name. Several new business process and technological advances such as Electronic Bill Presentment and Payment (EBPP), handheld access devices such as Personal Digital Assistants (PDAs), Internet Telephone and Wireless Communication channels and phones are emerging in the US market. A few banks have become Internet Service Providers (ISPs), and banks may become Internet portal sites and online service providers in the near future. Reliance on third party vendors is a common feature of electronic banking ventures of all sizes and degrees of sophistication in the US.

Currently, payments made over the Internet are almost exclusively conducted through existing payment instruments and networks. For retail e-commerce in the US, most payments made over the Internet are currently completed with credit cards and are cleared and settled through existing credit card clearing and settlement systems. Efforts are under way to make it easier to use debit cards, cheques and the Automated Clearing House (ACH) to make payments over the Internet. Versions of e-money, smart cards, e-cheques and other innovations are being experimented with to support retail payments over the Internet.

There is a matrix of legislation and regulations within the US that specifically codifies the use of and rights associated with the Internet and e-commerce in general, and electronic banking and Internet banking activities in particular. Federal and state laws, regulations, and court decisions, and self-regulation among context of electronic delivery. In addition, the Federal Reserve Board has issued a request for comment on revised proposals that would permit electronic delivery of federally mandated disclosures under the five consumer protection regulations of the FRB (Regulations B, DD, E, M & Z).

The Interpretive Ruling of the Office of the Comptroller of Currency (OCC) authorizes a national bank to 'perform, provide or deliver through electronic means and facilities any activity, functions, product or service that it is otherwise authorized to perform, provide or deliver'. The concerns of the Federal Reserve are limited to ensuring that Internet banking and other electronic banking services are implemented with proper attention to security, the safety and soundness of the bank, and the protection of the banks' customers. Currently, all banks, whether they are 'Internet only' or traditional banks must apply for a charter according to existing guidelines.

The five federal agencies - Federal Deposit Insurance Corporation (FDIC), Federal Reserve System (FRS), Office of the Comptroller of Currency (OCC), Office of Thrift Supervision (OTS) and the National Credit Union Association (NCUA) supervise more than 20,000 institutions. In addition, each state has a supervisory agency for the banks that it charters. Most financial institutions in the US face no prerequisite conditions or notification requirements for an existing banking institution to begin electronic banking activities.

For these banks, supervisors gather information on electronic banking during routine annual examination. Newly chartered Internet banks are subject to the standard chartering procedures. For thrift institutions, however, OTS has instituted a 30-day advance notification requirement for thrift institutions that plan to establish a transactional web site. A few State banking departments have instituted a similar notification requirement for transactional Internet banking web sites.

Supervisory policy, licensing, legal requirements and consumer protection are generally similar for electronic banking and traditional banking activities. Internet banks are also subject to the same rules, regulations and policy statement as traditional banks. However, in response to the risks posed by electronic banking, federal banking agencies have begun to issue supervisory guidelines and examination procedures for examiners who review and inspect electronic banking applications. Although specialized banking procedures are used in some areas of Internet banking activities, the existing information technology examination framework that addresses access controls, information security, business recovery and other risk areas generally continues to be applicable. To assist supervisors in monitoring the expansion of Internet banking, state chartered and national banks have been required since June 1999 to report their websites' 'Uniform Resource Locators' (URL) in the Quarterly Reports of Financial Condition that are submitted to supervisors.

In addition, examiners review the potential for reputational risk associated with web-site information or activities, the potential impact of various Internet strategies on an institution's financial condition, and the need to monitor and manage outsourcing relationships. To address these risks, the OCC is developing specific guidance for establishing 'Internet only' banks within the US. The Banking Industry Technology Secretariat recently announced the formation of a security lab to test and validate the security of software and hardware used by banking organizations.

If a bank is relying on a third party provider, it is accepted that it should be able to understand the provided information security programme to effectively evaluate the security system's ability to protect bank and customer data. Examination of service providers' operations, where necessary, is conducted by one or more Federal banking agencies pursuant to the Bank Services Company Act, solely to support supervision of banking organizations.

The Federal Financial Institutions Examination Council (FFIEC) introduced the Information Systems (IS) rating system to be used by federal and state regulators to assess uniformly financial and service provider risks introduced by information technology and to identify those institutions and service providers requiring special supervisor attention. The FFIEC has recently renamed the system as Uniform Rating System for IT (URSIT), which has enhanced the audit function. The importance of risk management procedure has been reinforced under the revised system.

Some characteristics of e-money products such as their relative lack of-physical bulk, their potential anonymity and the possibility of effecting fast and remote transfers make them more susceptible than traditional systems to money laundering activities. The OCC guidelines lay down an effective 'know your customer' policy. Federal financial institutions, regulators, Society for Worldwide Inter-bank Financial Telecommunications (SWIFT) and Clearing House Inter-bank Payment System (CHIPS) have issued statements encouraging participants to include information on originators and beneficiaries.[11]

2.2.2 United Kingdom [U.K.]: [18]

Most banks in U.K. are offering transactional services through a wider range of channels including Wireless Application Protocol (WAP), mobile phone and T.V. A number of non-banks have approached the Financial Services Authority (FSA) about charters for virtual banks or 'clicks and mortar' operations. There is a move towards banks establishing portals.

The Financial Services Authority (FSA) is neutral on regulations of electronic banks. The current legislation, viz. the Banking Act 1987 and the Building Societies Act, provides it with the necessary powers and the current range of supervisory tools. A new legislation, the Financial Services and Market Bill, offers a significant addition in the form of an objective requiring the FSA to promote public understanding of the financial system. There is, therefore, no special regime for electronic banks. A draft Electronic Banking Guidance for supervisors has, however, been developed.

A guide to Bank Policy has also been published by the FSA which is technology neutral, but specifically covers outsourcing and fraud. The FSA also maintains bilateral discussions with other national supervisors and monitors developments in the European Union (EU) including discussions by the Banking Advisory Committee and Group de Contract. New legislation on money laundering has been proposed and both the British Bankers Association and the FSA have issued guidance papers in this regard.

The FSA is actively involved in the Basle Committee e-banking group which has identified authorization, prudential standards, transparency, privacy, money laundering and cross border provision as issues where there is need for further work. The FSA has also been supporting the efforts of the G7 Financial Stability Forum, which is exploring common standards for financial market, which is particularly relevant to the Internet, which reaches across all borders.

The Financial Services and Markets Bill will replace current powers under the 1987 Banking Act giving the FSA statutory authority for consumer protection and promotion of consumer awareness. Consumer compliance is required to be ensured via desk based and on site supervision. The FSA has an Authorization and Enforcement Division, which sees if web sites referred to them are in violation of U.K. laws.

The FSA has issued guidelines on advertising in U.K. by banks for deposits, investments and other securities, which apply to Internet banking also. The guidelines include an Appendix on Internet banking. The FSA's supervisory policy and powers in relation to breaches in the advertising code (viz. invitation by any authorized person to take a deposit within U.K., fraudulent inducements to make a deposit, illegal use of banking names and descriptions, etc.) are the same for Internet banking as they are for conventional banking. The FSA does not regard a bank authorized overseas, which is targeting potential depositors in its home market or in third countries as falling within U.K. regulatory requirements solely by reason of its web site being accessible to Internet users within the U.K., as the advertisements are not aimed at potential U.K. depositors. [12]

2.2.3 Scandinavia: [19]

Swedish and Finnish markets lead the world in terms of Internet penetration and the range and quality of their online services. Merita Nordbanken (MRB) (now Nordic Bank Holding, a merger between Finland's Merita and Nord banker of Sweden) leads in "log-ins per month" with 1.2 million Internet customers, and its penetration rate in Finland (around 45%) is among the highest in the world for a bank of 'brick and mortar' origin. Standinaviska Easkilda Banken (SEB) was Sweden's first Internet bank, having gone on-line in December 1996. It has 1,000 corporate clients for its Trading Station - an Internet based trading mechanism for forex dealing, stock-index futures and Swedish treasury bills and government bonds. Swed bank, is another large sized Internet bank. Almost all of the approximately 150 banks operating in Norway had established "net banks".

In Denmark, the Internet banking service of Den Danske offers funds transfers, bill payments, etc. The basic on-line activity is paying bills. Swed bank was the first bank in the world to introduce Electronic Bill Presentment and Payment (EBPP) and now handles 2 million bill payment a month. E-shopping is another major Internet banking service. MNB has an on-line "mall" of, more than 900 shops, which accepts its "Solo" payment system. Swed bank has a similar system called "Direct".

Besides using advanced encryption technology, the Scandenavian banks have adopted a basic but effective system known as "challenge response logic", which involves a list of code numbers sent to every online client and used in sequence, in combination with their password or PIN. This gives each transaction a unique code, and has so far proved safe. Some banks use even more sophisticated versions of the same technique. It is not a common practice to use third party vendors for services.

In Sweden, no formal guidance has been given to examiners by the Sveriges bank on e-banking. General guidelines apply equally to Internet banking activities. Contractual regularization between customers and the bank is a concern for regulators and is being looked into by the authorities.

The role of the Bank of Finland (Suomen Parkki) has been, as part of general oversight of financial markets in Finland, mainly to monitor the ongoing development of Internet banking without active participation. Numerous issues concerning Internet banking have, however, been examined by the Bank of Finland.

All Internet banking operating from a Norwegian platform are subject to all regular banking regulations, just as any other bank. As part of the standard regulation, there is also a specific regulation on the banks' use of IT. This regulation dates from 1992 when Internet banking was not the main issue, but it covers all IT systems, including Internet banking. The regulation secures that banks' purchase, development, use and phase out of IT systems is conducted in a safe and controlled manner.

An Act relating to Payment systems defines payment systems as those which are based on standardized terms for transfer of funds from or between customer accounts in banks/financial undertakings when the transfer is based on use of payment cards, numeric codes or any other form of independent user identification.

Internet banking is covered by this regulation. The Banking, Insurance and Securities Commission may order for implementation of measures to remedy the situation if there is a violation of provisions.

In addition to their national laws, countries in Europe are also expected to implement European Union (EU) directives. In 1995, the EU passed a Europe-wide Data Protection Directive aimed at granting individuals greater protection from abuses of their personal information. It also passed the Telecommunications Directive that prescribes special protection in relation to telephones, digital TVs, mobile communications, etc. Every EU country is to have a privacy commissioner to enforce the regulations as they apply within the EU. The EU directive on electronic signature is also required to be implemented in national laws.[13]

2.2.4 Australia: [20]

Internet Banking in Australia is offered in two forms: web-based and through the provision of proprietary software. Initial web-based products have focused on personal banking whereas the provision of proprietary software has been targeted at the business/corporate sector. Most Australian-owned banks and some foreign subsidiaries of banks have transactional or interactive web-sites. Online banking services range from FIs' websites providing information on financial products to enabling account management and financial transactions.

Customer services offered online include account monitoring (electronic statements, real-time account balances), account management (bill payments, funds transfers, applying for products on-line) and financial transactions (securities trading, foreign currency transactions).

Electronic Bill Presentment and Payment (EBPP) is at an early stage. Features offered in proprietary software products (enabling business and corporation customers to connect to the financial institutions (via dial-up/leased line/extranet) include account reporting, improved reconciliation, direct payments, payroll functionality and funds transfer between accounts held at their own or other banks.

Apart from closed payment systems (involving a single payment-provider), Internet banking and e-commerce transactions in Australia are conducted using long-standing payment instruments and are cleared and settled through existing clearing and settlement system. Banks rely on third party vendors or are involved with outside providers for a range of products and services including e-banking. Generally, there are no 'virtual' banks licensed to operate in Australia.

The Electronic Transactions Act, 1999 provides certainty about the legal status of electronic transactions and allows for Australians to use the Internet to provide Commonwealth Departments and agencies with documents which have the same legal status as traditional paperwork.

The Australian Securities and Investments Commission (ASIC) is the Australian regulator with responsibility for consumer aspects of banking, insurance and superannuation and as such, it is responsible for developing policy on consumer protection issues relating to the Internet and e-commerce.

ASIC currently has a draft proposal to expand the existing Electronic Funds Transfer Code of Conduct (a voluntary code that deals with transactions initiated using a card and a PIN) to cover all forms of consumer technologies, including stored value cards and other new electronic payment products. Australia's anti-money laundering regulator is the Australian Transaction Reports and Analysis Centre (AUSTRAC).

Responsibility for prudential supervisory matters lies with the Australian Prudential Regulation Authority (APRA). APRA does not have any Internet specific legislation, regulations or policy, and banks are expected to comply with the established legislation and prudential standards.

APRA's approach to the supervision of e-commerce activities, like the products and services themselves, is at an early stage and is still evolving. APRA's approach is to visit institutions to discuss their Internet banking initiatives. However, APRA is undertaking a survey of e-commerce activities of all regulated financial institutions. The growing reliance on third party or outside providers of e-banking is an area on which APRA is increasingly focusing. [14]

2.2.5 New Zealand: [21]

Major Banks offer Internet banking service to customers; operate as a division of the bank rather than as a separate legal entity. Reserve Bank of New Zealand applies the same approach to the regulation of both Internet banking activities and traditional banking activities. There are however, banking supervision regulations that apply only to Internet banking. Supervision is based on public disclosure of information rather than application of detailed prudential rules. These disclosure rules apply to Internet banking activity also. [15]

2.2.6 Singapore: [22]

The Monetary Authority of Singapore (MAS) has reviewed its current framework for licensing, and for prudential regulation and supervision of banks, to ensure its relevance in the light of developments in Internet banking, either as an additional channel or in the form of a specialized division, or as stand-alone entities (Internet Only Banks), owned either by existing banks or by new players entering the banking industry. The existing policy of MAS already allows all banks licensed in Singapore to use the Internet to provide banking services.

MAS are subjecting Internet banking, including IOBs, to the same prudential standards as traditional banking. It will be granting new licenses to banking groups incorporated in Singapore to set up bank subsidiaries if they wish to pursue new business models and give them flexibility to decide whether to engage in Internet banking through a subsidiary or within the bank (where no additional license is required). MAS also will be admitting branches of foreign incorporated IOBs within the existing framework of admission of foreign banks.

As certain types of risk are accentuated in Internet banking, a risk - based supervisory approach, tailored to individual banks' circumstances and strategies, is considered more appropriate by MAS than "one-size-fits-all" regulation. MAS requires public disclosures of such undertakings, as part of its requirement for all banks and enhance disclosure of their risk management systems. It is issuing a consultative document on Internet banking security and technology risk management. In their risk management initiatives for Internet banking relating to security and technology related risks, banks should:

a) Implement appropriate workflow, authenticated process and control procedures surrounding physical and system access.
b) Develop, test, implement and maintain disaster recovery and business contingency plans.
c) Appoint an independent third party specialist to assess its security and operations.
d) Clearly communicate to customers their policies with reference to rights and responsibilities of the bank and customer, particularly issues arising from errors in security systems and related procedures.

For liquidity risk, banks, especially IOBs, should establish robust liquidity contingency plans and appropriate Asset-Liability Management systems. As regards operational risk, banks should carefully manage outsourcing of operations, and maintain comprehensive audit trails of all such operations. As far as business risk is concerned, IOBs should maintain and continually update a detailed system of performance measurement.

MAS encourages financial institutions and industry associations such as the Associations of Banks in Singapore (ABS) to play a proactive role in educating consumers on benefits and risks on new financial products and services offered by banks, including Internet banking service.[16]

2.2.7 Hong Kong: [23]

There has been a spate of activity in Internet banking in Hong Kong. Two virtual banks are being planned. It is estimated that almost 15% of transactions are processed on the Internet. During the first quarter of 2000, seven banks have begun Internet services. Banks are participating in strategic alliances for e-commerce ventures and are forming alliances for Internet banking services delivered through Jetco (a bank consortium operating an ATM network in Hong Kong). A few banks have launched transactional mobile phone banking earlier for retail customers.

The Hong Kong Monetary Authority (HKMA) requires that banks must discuss their business plans and risk management measures before launching a transactional website. HKMA has the right to carry out inspections of security controls and obtain reports from the home supervisor, external auditors or experts commissioned to produce reports. HKMA is developing specific guidance on information security with the guiding principle that security should be "fit for purpose".

HKMA requires that risks in Internet banking system should be properly controlled. The onus of maintaining adequate systems of control including those in respect of Internet banking ultimately lies with the institution itself. Under the Seventh Schedule to the Banking ordinance, one of the authorization criteria is the requirement to maintain adequate accounting system and adequate systems control. Banks should continue to acquire state-of-the art technologies and to keep pace with developments in security measures.

The HKMA's supervisory approach is to hold discussions with individual institutions who wish to embark on Internet banking to allow them to demonstrate how they have properly addressed the security systems before starting to provide such services, particularly in respect of the following – (i) encryption by industry proven techniques of data accessible by outsiders, (ii) preventive measures for unauthorized access to the bank's internal computer systems, (iii) set of comprehensive security policies and procedures, (iv) reporting to HKMA all security incidents and adequacy of security measures on a timely basis.

At present, it has not been considered necessary to codify security objectives and requirements into a guideline. The general security objectives for institutions intending to offer Internet banking services should have been considered and addressed by such institutions.

HKMA has issued guidelines on 'Authorization of Virtual Banks' under Section 16(10) of the Banking Ordinance under which (i) the HKMA will not object to the establishment of virtual banks in Hong Kong provided they can satisfy the same prudential criteria that apply to conventional banks, (ii) a virtual bank which wishes to carry on banking business in Hong Kong must maintain a physical presence in Hong Kong; (iii) a virtual bank must maintain a level of security which is appropriate to the type of business which it intends to carry out. A copy of report on security of computer hardware, systems, procedures, controls etc. from a qualified independent expert should be provided to the HKMA at the time of application, (iv) a virtual bank must put in place appropriate policies, procedures and controls to meet the risks involved in the business; (v) the virtual bank must set out clearly in the terms and conditions for its service what are the rights and obligations of its customers (vi) Outsourcing by virtual banks to a third party service provider is allowed, provided HKMA's guidelines on outsourcing are complied with. There are principles applicable to locally incorporated virtual banks and those applicable to overseas-incorporated virtual banks.

Consumer protection laws in Hong Kong do not apply specifically to e-banking but banks are expected to ensure that their e-services comply with the relevant laws. The Code of Banking Practice is being reviewed to incorporate safeguards for customers of e-banking.

Advertising for taking deposits to a location outside Hong Kong is a violation unless disclosure requirements are met. Consideration is being given as to whether this is not too onerous in the context of the global nature of the Internet.

Recognizing the relevance of Public Key Infrastructure (PKI) in Hong Kong to the development of Internet banking and other forms of e-commerce, the government of Hong Kong has invited the Hong Kong Postal Authority to serve as public Certificate Authority (CA) and to establish the necessary PKI infrastructure.

There is no bar, however, on the private sector setting up CAs to serve the specific needs of individual networks. There should be cross-references and mutual recognition of digital signatures among CAs. The Government is also considering whether and, if so, how the legal framework should be strengthened to provide firm legal basis for electronic transactions (particularly for digital signatures to ensure non-repudiation of electronic messages and transactions). [17]

2.2.8 Japan: [24]

Banks in Japan are increasingly focusing on e-banking transactions with customers. Internet banking is an important part of their strategy. While some banks provide services such as inquiry, settlement, purchase of financial products and loan application, others are looking at setting up finance portals with non-finance business corporations. Most banks use outside vendors in addition to in-house services.

The current regulations of the Bank of Japan on physical presence of bank branches are undergoing modifications to take care of licensing of banks and their branches with no physical presence. The Report of the Electronic Financial Services Study Group (EFSSG) has made recommendations regarding the supervision and regulation of electronic financial services. Financial institutions are required to take sufficient measures for risk management of service providers and the authorities are required to verify that such measures have been taken. Providing information about non-financial businesses on a bank web site is not a violation as long as it does not constitute a business itself.

With respect to consumer protection it is felt that guidance and not regulations should encourage voluntary efforts of individual institutions in this area. Protection of private information, however, is becoming a burning issue in Japan both within and outside the field of e-banking. Japanese banks are currently requested to place disclosure publications in their offices (branches) by the law. However, 'Internet Only banks' are finding it difficult to satisfy this requirement. The Report of the EFSSG recommends that financial service providers that operate transactional website should practice online disclosure through electronic means at the same timing and of equivalent contents as paper based disclosure. They should also explain the risks and give customers a fair chance to ask queries. The Government of Japan intends to introduce comprehensive Data Protection Legislation in the near future. There are no restrictions or requirements on the use of cryptography. The Ministry of International Trade and Industry (MITI)'s approval is required to report encryption technology.

World over, electronic banking is making rapid strides due to evolving communication technology. Penetration of Internet banking is increasing in most countries. Wireless Application Protocol (WAP) is an emerging service which banks worldwide are also offering. The stiff competition in this area exposes banks to substantial risks. The need is being felt overseas that transparency and disclosure requirements should be met by the e-banking community. While existing regulations and legislations applicable to traditional banking are being extended to banks' Internet banking and electronic banking services, it is recognized that Internet security, customer authentication and other issues such as technology outsourcing pose unique risks.

Central Banks worldwide are addressing such issues with focused attention. Special legislations and regulations are being framed by the regulators and supervisors for proper management of the different types of risks posed by these services. The reliance on outsourcing is an area where overseas regulators and supervisors are focusing their attention, with banks having to regularly review and test business continuity, recovery and incidence response plans in order to maintain their reputation of trust. Consumer protection and data privacy are areas which assume great significance when banking transactions are carried over a medium as insecure as the Internet.

Many countries are looking at special consumer protection/data privacy legislation for an e-commerce environment. The presence of 'virtual banks' or 'Internet only banks' and the licensing requirements required for such entities are also areas which are being looked into by overseas authorities.

There has also been co-operation among the regulators and supervisors to meet the challenges of 'virtual' cross border e-banking, particularly in the light of the possibility of increased money laundering activities through the medium of Internet. Internet banking is universally seen as a welcome development, and efforts are being made to put in place systems to manage and control the risks involved without restricting this service. [18]

2.3 Internet Banking: The Indian Scenario:

"Use of the Internet for banking has seen a massive rise in the 2010-11 survey, taking the overall number of bank consumers who use the Net to close 7% of the total bank account holders -- a seven-fold jump since 2007 -- even as for the first time in the past 13 years, branch banking has come down by a full 15 percentage points during the same period

2.3.1 The entry of Indian banks into Net Banking: [25]

Internet banking, both as a medium of delivery of banking services and as a strategic tool for business development, has gained wide acceptance internationally and is fast catching up in India with more and more banks entering the fray. India can be said to be on the threshold of a major banking revolution with net banking having already been unveiled. A recent questionnaire to which 46 banks responded, has revealed that at present, 11 banks in India are providing Internet banking services at different levels, banks propose to offer Internet banking in near future while the remaining 13 banks have no immediate plans to offer such facility.

At present, the total Internet users in the country are estimated at 9 lakh. However, this is expected to grow exponentially to 90 lakh by 2003. Only about 1% of Internet users did banking online in 1998. This increased to 16.7% in March 2000. The growth potential is, therefore, immense. Further incentives provided by banks would dissuade customers from visiting physical branches, and thus get 'hooked' to the convenience of arm-chair banking. The facility of accessing their accounts from anywhere in the world by using a home computer-with Internet connection, is particularly fascinating to Non-Resident Indians and High Net worth Individuals having multiple bank accounts.

Costs of banking service through the Internet form a fraction of costs through conventional methods. Rough estimates assume teller cost at Re.1 per transaction, ATM transaction cost at 45 paise, phone banking at 35 paise, debit cards at 20 paise and Internet banking at 10 paise per transaction. The cost-conscious banks in the country have therefore actively considered use of the Internet as a channel for providing services. Fully computerized banks, with better management of their customer base are in a stronger position to cross-sell their products through this channel. [19]

2.3.2 Products and services offered: [26]

Banks in India are at different stages of the web-enabled banking cycle. Initially, a bank, which is not having a web site, allows its customer to communicate with it through an e-mail address; communication is limited to a small number of branches and offices which have access to this e-mail account. As yet, many scheduled commercial banks in India are still in the first stage of Internet banking operations.

With gradual adoption of Information Technology, the bank puts up a web-site that provides general information on the banks, its location, services available e.g. loan and deposits products, application forms for downloading and e-mail option for enquiries and feedback. It is largely a marketing or advertising tool. For example, Vijaya Bank provides information on its web-site about its NRI and other services. Customers are required to fill in applications on the Net and can later receive loans or other products requested for at their local branch. A few banks provide the customer to enquire into his demat account (securities/shares) holding details, transaction details and status of instructions given by him. These web sites still do not allow online transactions for their customers.

Some of the banks permit customers to interact with them and transact electronically with them. Such services include request for opening of accounts, requisition for cheque books, stop payment of cheques, viewing and printing statements of accounts, movement of funds between accounts within the same bank, querying on status of requests, instructions for opening of Letters of Credit and Bank Guarantees etc.

These services are being initiated by banks like ICICI Bank Ltd., HDFC Bank Ltd. Citibank, Global Trust Bank Ltd., UTI Bank Ltd., Bank of Madura Ltd., Federal Bank Ltd. etc. Recent entrants in Internet banking are Allahabad Bank (for its corporate customers through its 'Allnet' service) and Bank of Punjab Ltd. State Bank of India has announced that it will be providing such services soon. Certain banks like ICICI Bank Ltd., have gone a step further within the transactional stage of Internet banking by allowing transfer of funds by an account holder to any other account holder of the bank.

Some of the more aggressive players in this area such as ICICI Bank Ltd., HDFC Bank Ltd., UTI Bank Ltd., Citibank, Global Trust Bank Ltd. and Bank of Punjab Ltd. offer the facility of receipt, review and payment of bills on-line. These banks have tied up with a number of utility companies. The 'Infinity' service of ICICI Bank Ltd. Also allows online real time shopping mall payments to be made by customers. HDFC Bank Ltd. has made e-shopping online and real time with the launch of its payment gateway. It has tied up with a number of portals to offer business-to-consumer (B2C) ecommerce transactions. The first online real time e-commerce credit card transaction in the country was carried out on the Easy3shoppe.com shopping mall, enabled by HDFC Bank Ltd. on a VISA card.

Banks like ICICI Bank Ltd., HDFC Bank Ltd. etc. are thus looking to position themselves as one stop financial shops. These banks have tied up with computer training companies, computer manufacturers, Internet Services Providers and portals for expanding their Net banking services, and widening their customer base. ICICI Bank Ltd. has set up a web based joint venture for on-line distribution of its retail banking products and services on the Internet, in collaboration with Satyam Infoway, a private ISP through a portal named as icicisify.com. The customer base of www.satyamonline.com portal is also available to the bank. Setting up of Internet kiosks and permeation through the cable television route to widen customer base are other priority areas in the agendas of the more aggressive players. Centurion Bank Ltd. has taken up equity stake in the teauction.com portal, which aims to bring together buyers, sellers, registered brokers, suppliers and associations in the tea market and substitute their physical presence at the auctions announced.

Banks providing Internet banking services have been entering into agreements with their customers setting out the terms and conditions of the services. The terms and conditions include information on the access through user-id and secret password, minimum balance and charges, authority to the bank for carrying out transactions performed through the service, liability of the user and the bank, disclosure of personal information for statistical analysis and credit scoring also, non-transferability of the facility, notices and termination, etc.

The race for market supremacy is compelling banks in India to adopt the latest technology on the Internet in a bid to capture new markets and customers. HDFC Bank Ltd. with its 'Freedom- the e-Age Saving Account' Service, Citibank with Suvidha and ICICI Bank Ltd. with its Mobile Commerce service have tied up with cellphone operators to offer Mobile Banking to their customers. Global Trust Bank Ltd. has also announced that it has tied up with cellular operators to launch mobile banking services. Under Mobile Banking services, customers can scan their accounts to seek balance and payments status or instruct banks to issue cheques, pay bills or deliver statements of accounts. It is estimated that by 2003, cellular phones will have become the premier Internet access device, outselling personal computers. Mobile banking will further minimize the need to visit a bank branch. [20]

2.3.3 The Future Scenario: Internet Banking in India: [27]

Compared to banks abroad, Indian banks offering online services still have a long way to go. For online banking to reach a critical mass, there has to be sufficient number of users and the sufficient infrastructure in place. The 'Infinity' product of ICICI Bank Ltd. gets only about 30,000 hits per month, with around 3,000 transactions taking place on the Net per month through this service.

Though various security options like line encryption, branch connection encryption, firewalls, digital certificates, automatic signoffs, random pop-ups and disaster recovery sites are in place or are being looked at, there is as yet no Certification Authority in India offering Public Key Infrastructure which is absolutely necessary for online banking. The customer can only be assured of a secured conduit for its online activities if an authority certifying digital signatures is in place. The communication bandwidth available today in India is also not enough to meet the needs of high priority services like online banking and trading.

Banks offering online facilities need to have an effective disaster recovery plan along with comprehensive risk management measures. Banks offering online facilities also need to calculate their downtime losses, because even a few minutes of downtime in a week could mean substantial losses. Some banks even today do not have uninterrupted power supply unit or systems to take care of prolonged power breakdown. Proper encryption of data and effective use of passwords are also matters that leave a lot to be desired. Systems and processes have to be put in place to ensure that errors do not take place.

Users of Internet Banking Services are required to fill up the application forms online and send a copy of the same by mail or fax to the bank. A contractual agreement is entered into by the customer with the bank for using the Internet banking services. In this way, personal data in the applications forms is being held by the bank providing the service. The contract details are often one-sided, with the bank having the absolute discretion to amend or supplement any of the terms at any time.

For these reasons domestic customers for whom other access points such as ATMs, tele-banking, personal contact, etc. are available, are often hesitant to use the Internet banking services offered by Indian banks. Internet Banking, as an additional delivery channel, may, therefore, be attractive / appealing as a value added service to domestic customers. Non-resident Indians for whom it is expensive and time consuming to access their bank accounts maintained in India find net banking very convenient and useful.

The Internet is in the public domain whereby geographical boundaries are eliminated. Cyber crimes are therefore difficult to be identified and controlled. In order to promote Internet banking services, it is necessary that the proper legal infrastructure is in place. Government has introduced the Information Technology Bill, which has already been notified in October 2000. Section 72 of the Information Technology Act, 2000 casts an obligation of confidentiality against disclosure of any electronic record, register, correspondence and information, except for certain purposes and violation of this provision is a criminal offence.

Notification for appointment of Authorities to certify digital signatures, ensuring confidentiality of data, is likely to be issued in the coming months. Comprehensive enactments like the Electronic Funds Transfer Act in U.K. and data protection rules and regulations in the developed countries are in place abroad to prevent unauthorized access to data, malafide or otherwise, and to protect the individual's rights of privacy. The legal issues are, however, being debated in our country and it is expected that some headway will be made in this respect in the near future.

Notwithstanding the above drawbacks, certain developments taking place at present, and expected to take place in the near future, would create a conducive environment for online banking to flourish. For example, Internet usage is expected to grow with cheaper bandwidth cost. The Department of Telecommunications (DoT) is moving fast to make available additional bandwidth, with the result that Internet access will become much faster in the future. This is expected to give a fillip to Internet banking in India.

The proposed setting up of a Credit Information Bureau for collecting and sharing credit information on borrowers of lending institutions online would give a fillip to electronic banking. The deadline set by the Chief Vigilance Commissioner for computerization of not less than 70 percent of the bank's business by end of January 2001 has also given a greater thrust to development of banking technology. The recommendations of the Vasudevan Committee on Technological Upgradation of Banks in India have also been circulated to banks for implementation. In this background, banks are moving in for technological Upgradation on a large scale. Internet banking is expected to get a boost from such developments.

Reserve Bank of India has taken the initiative for facilitating real time funds transfer through the Real Time Gross Settlement (RTGS) System. Under the RTGS system, transmission, processing and settlements of the instructions will be done on a continuous basis. Gross settlement in a real time mode eliminates credit and liquidity risks. Any member of the system will be able to access it through only one specified gateway in order to ensure rigorous access control measures at the user level. The system will have various levels of security, viz., Access security, 128 bit cryptography, firewall, certification etc. Further, Generic Architecture (**see fig. 2**), both domestic and cross border, aimed at providing inter-connectivity across banks has been accepted for implementation by RBI. Following a reference made this year, in the Monetary and Credit Policy statement of the Governor, banks have been advised to develop domestic generic model in their computerization plans to ensure seamless integration. The abovementioned efforts would enable online banking to become more secure and efficient.

With the process of dematerialization of shares having gained considerable ground in recent years, banks have assumed the role of depository participants. In addition to customers' deposit accounts, they also maintain demat accounts of their clients. Online trading in equities is being allowed by SEBI. This is another area which banks are keen to get into. HDFC Bank Ltd., has tied up with about 25 equity brokerages for enabling third party transfer of funds and securities through its business-to-business (B2B) portal, 'e-Net'. Demat account holders with the bank can receive securities directly from the brokers' accounts. The bank has extended its web interface to the software vendors of National Stock Exchange through a tie-up with NSE.IT – the infotech arm of the exchange. The bank functions as the payment bank for enabling funds transfer from its customers' account to brokers' accounts. The bank is also setting up a net broking arm, HDFC Securities, for enabling trading in stocks through the web. The focus on capital market operations through the web is based on the bank's strategy on tapping customers interested in trading in equities through the Internet. Internet banking thus promises to become a popular delivery channel not only for retail banking products but also for online securities trading.

An upcoming payment gateway is being developed by ICICI and Global Tele System, which will enable customers to transfer funds to banks which are part of the project. Transfer of funds can be made through credit/debit/ smart cards and cheques, with the central payment switch enabling the transactions. Banks are showing interest in this new concept, which will facilitate inter-bank funds transfers and other e-commerce transactions, thus highlighting the role of banks in e-commerce as intermediaries between buyers and sellers in the whole payment process.

WAP (Wireless Application Protocol) telephony is the merger of mobile telephony with the Internet. It offers two-way connectivity, unlike Mobile Banking where the customer communicates to a mailbox answering machine. Users may surf their accounts, download items and transact a wider range of options through the cellphone screen. WAP may provide the infrastructure for P2P (person to person) or P2M (person to merchant) payments. It would be ideal for transactions that do not need any cash backup, such as online investments. Use of this cutting edge technology could well determine which bank obtains the largest market share in electronic banking. IDBI Bank Ltd. has recently launched its WAP- based mobile phone banking services (offering facilities such as banking enquiry, cheque book request, statements request, details of the bank's products etc).

At present, there are only 2.6 phone connections per 100 Indians, against the world average of 15 connections per 100. The bandwidth capacity available in the country is only 3.2 gigabits per second, which is around 60% of current demand. Demand for bandwidth is growing by 350% a year in India. With the help of the latest technology, Indian networks will be able to handle 40 gigabits of Net traffic per second (as compared to 10 gigabits per second in Malaysia). Companies like Reliance, Bharti Telecom and the Tata Group are investing billions of rupees to build fibre optic lines and telecom infrastructure for data, voice and Internet telephony.

The online population has increased from just 500,000 in 1998 to 5 million in 2000. By 2015, the online population is expected to reach 70 million. IT services is a $1.5 billion industry in India growing at a rate of 55% per annum. Keeping in view all the above developments, Internet banking is likely to grow at a rapid pace and most banks will enter into this area soon. Rapid strides are already being made in banking technology in India and Internet banking is a manifestation of this. Every day sees new tie-ups, innovations and strategies being announced by banks. State Bank of India has recently announced its intention to form an IT subsidiary. A sea change in banking services is on the cards. It would, however, be essential to have in place a proper regulatory, supervisory and legal framework, particularly as regards security of transactions over the Net, for regulators and customers alike to be comfortable with this form of banking.

2.4 Internet Banking and its various types: [28]

Currently, there are three basic kinds of Internet banking that are being employed in the market place:

Information:

This is the most basic level of Internet banking. The bank has marketing information about its products and services on a stand - alone server. This level of Internet banking service can be provided by the bank itself or by sourcing it out. Since the server or Web site may be vulnerable to alteration, appropriate controls must therefore be in place to prevent unauthorized alterations to data in the server or web site.

Communication:

This type of Internet banking allows interaction between the bank's systems and the customer. It may be limited to electronic mail, account inquiry, loan applications, or static file updates. The risk is higher with this configuration than with the earlier system and therefore appropriate controls need to be in place to prevent, monitor, and alert management of any unauthorized attempt to access bank's internal network and computer systems. Under this system the client makes a request to which the bank subsequently responds.

Transaction:

Under this system of Internet banking customers are allowed to execute transactions. Relative to the information and communication types of Internet banking, this system possesses the highest level of risk architecture and must have the strongest controls. Customer transactions can include accessing accounts, paying bills, transferring funds, etc. These possibilities demand very stringent security.

2.4.1 Types of Services Available: [29]

Net banking is a web-based service that enables the banks authorized customers to access their account information. It allows the customers to log on to the banks website with the help of bank's issued identification and personal identification number (PIN).

The banking system verifies the user and provides access to the requested services, the range of products and service offered by each bank on the internet differs widely in their content. Most banks offer net banking as a value-added service. Net banking has also led to the emergent of new banks, which operate only through the internet and do not exists physically, Such banks are called "virtual" banks or "Internet Only" banks. A couple of years ago, there was a belief even among bankers that customers opening new accounts wanted the online banking facility, just to 'feel good' and very few of them actually used that services.

Today, bankers believe that the trend from 'nice to have' is changing to 'need to have' .after all it depends on how busy a person is. Services provided through Internet Banking 1) account information 2) E-cheques (Online Fund Transfer) 3) Bill Payment Service 4) Requests and Intimations 5) Demat Account share trading. Through Internet banking, customers can not only get account balance and see statements of account online but they can also transfer funds, order demand drafts, pay utility bills etc. Following types of main transactions or operations can be performed through. Internet banking:

Account Information:

Provides summary of all bank accounts. Allow transaction tracking which enables retrieval of transaction details based on cheque number, transaction amount, and date. Provide account statement and transaction reports used on user-defined criteria. Customers can even download and print the statement of accounts.

Funds Transfer (E-Cheque):

Customer can transfer funds: Transfer funds between accounts, even if they are in different branches' cities Customer can also transfer funds to any person having an account with the same bank anytime, anywhere, using third party funds transfer option.

Bill Presentment and Payment:

Banks Bill Payments is the easiest way to manage bills. A/c holder can pay their regular monthly bills i.e. telephone, electricity, mobile phone, insurance etc. at anytime, anywhere for free. Saves time and effort. Make bill payments at customer's convenience form their home or office. Lets a/c holders check their hill amount before it is debited form their account. No debits to account without their knowledge. No more missed deadlines, no more loss of interest - a/c holder can schedule their bills in advance, avoid missing the bill deadlines as well as earn extra interest on their money. Track payment history – all payments to a biller are stored automatically for future reference. No queuing up at collection centers or writing cheque anymore! Just a few clicks and customers account will be debited for the exact amount they ask.

Premium:

- Online Payment for Shopping done on Internet.
- Loan Applications.
- Standing Instructions.
- Request and Intimations.
- Financial Advice.
- Credit and Debit Cards.
- Investment Transactions.
- Customer Correspondence.
- Opening Accounts.
- Insurance.
- Other Value Added / Premium Services etc.

2.4.2 Mediums of E-banking: [Various products and services:] [30]

Electronic banking, also known electronic fund transfer (EFT), uses computer and electronic technology as a substitute for checks and other paper transactions. EFTs is initiated through devices like cards or codes that let you, or those you authorize, access your account.

Many financial institutions use ATM or debit cards and Personal Identification Numbers (PINs) for this purpose. Some use other forms of debit cards and personal Identification Numbers (PINs) for this purpose. Some use other forms of debit cards such as those that require, at the most, your signature or a scan. The federal Electronic Fund Transfer Act (EFT Act) covers some electronic consumer transactions.

Following are the electronic medium by which services are generally provided by the banks as a part of e-banking services.

1. Internet Banking
2. ATM (Automatic Teller Machine)
3. Phone Banking
4. Mobile Banking
5. Payment Cards (Debits/Credit Card)

All the above mediums provide services, which can be, also know as "any time any where banking". This facilitates the customer of the bank to operate their account from any corner of the world, without visiting local or any subsidiary branch of their banks. Efforts are made by the bank not only to provide the facility to the customer, but also to reduce the operational cost of the bank by providing e-banking services. So with this, banks have to employ less staff and still would be able to deliver service to the customer, round the corner.

2.4.3 Factors Responsible for Growth of Internet Banking: [31]

Numerous factors including competitive cost, customer service, and demographic considerations are motivating banks to evaluate their technology and assess their Internet banking strategies. The challenge for national banks is to make sure the savings from Internet banking technology more than offset the costs and risks associated with conducting business in cyberspace. Marketing strategies will vary as national banks seek to expand their markets and employ lower cost delivery channels. Examiners will need to understand the strategies used and technologies employed on a bank-by-bank basis to assess the risk. Evaluating a bank's data on the use of their Web sites, may help examiners determine the bank's strategic objectives, how well the bank is meeting its Internet banking product plan, and whether the business is expected to be profitable.

Competition:
Studies show that competitive pressure is the chief driving force behind increasing use of Internet banking technology, ranking ahead of cost reduction and revenue enhancement, in second and third place respectively. Banks see Internet banking as a way to keep existing customers and attract new ones to the bank.

Cost Efficiencies:
Banks can deliver banking services on the Internet at transaction costs far lower than traditional brick and mortar branches. The actual costs to execute a transaction will vary depending on the delivery channel used. The frequently quoted Booz - Allen and Hamilton study showed that the cost of a customer walking into the branch and using a teller is US$1.01, where as the cost of conducting the same transaction on the Internet is only a tenth of the cost. No doubt the ATM is considerably cheaper than a teller, but even so, the Internet is nearly 3 times cheaper than the ATM usage. In short, replacing a teller with an Internet channel should in theory, show a 10 fold increase in the distribution revenue for the bank. This reason alone should be sufficient for banks to encourage this form of distribution channel. However, banks should use care in making product decisions. Management should include in their decision making the development and ongoing costs associated with a new product or service, including the technology, marketing, maintenance, and customer support functions. This will help management exercise due diligence, make more informed decisions, and measure the Success of their business venture.

Geographical Reach:
Internet banking allows expanded customer contact through increased geographical reach and lower cost delivery channels. In fact some banks are doing business exclusively via the Internet. They do not have traditional banking offices and only reach their customers online. Other financial institutions are using the Internet as an alternative delivery channel to reach existing customers adds attract new customers.

Branding:
Relationship building is a strategic priority for many national banks. Internet banking technology and products can provide a means for national banks to develop and maintain an ongoing relationship with their customers by offering easy access to a broad array of products and services. By capitalizing on brand identification and by providing a broad array of financial services, banks hope to build customer loyalty, cross sell, and enhance repeat business.

Customer Demographics:
Internet banking allows national banks to offer a wide array of options to their banking customers. Some customers will rely on traditional branches to conduct their banking business. For many, this is the most comfortable way for them to transact their banking business. Those customers place a premium on person to person contact other customers are early adopters of new technologies that arrive in the marketplace. These customers were the first to obtain PCs and the first to employ them in conducting their banking business. The demographics of banking customers will continue to change.

Round the Clock Access:
Internet banking services are available on 24 x 7 basis to the customers without charging any extra cost from the customers. And one can access the bank from anywhere in the world at one's own convenience without owning your own PC.

2.5 Types of risks associated with Internet banking: [32]

A major driving force behind the rapid spread of i-banking all over the world is its acceptance as an extremely cost effective delivery channel of banking services as compared to other existing channels. However, Internet is not an unmixed blessing to the banking sector. Along with reduction in cost of transactions, it has also brought about a new orientation to risks and even new forms of risks to which banks conducting i-banking expose themselves.

Regulators and supervisors all over the world are concerned that while banks should remain efficient and cost effective, they must be conscious of different types of risks this form of banking entails and have systems in place to manage the same. An important and distinctive feature is that technology plays a significant part both as source and tool for control of risks. Because of rapid changes in information technology, there is no finality either in the types of risks or their control measures. Both evolve continuously. The thrust of regulatory action in risk control has been to identify risks in broad terms and to ensure that banks have minimum systems in place to address the same and that such systems are reviewed on a continuous basis in keeping with changes in technology. In the following paragraphs a generic set of risks are discussed as the basis for formulating general risk control guidelines, which this Group will address.

2.5.1 Operational Risk: [33]

Operational risk, also referred to as transactional risk is the most common form of risk associated with i-banking. It takes the form of inaccurate processing of transactions, non enforceability of contracts, compromises in data integrity, data privacy and confidentiality, unauthorized access / intrusion to bank's systems and transactions etc. Such risks can arise out of weaknesses in design, implementation and monitoring of banks' information system. Besides inadequacies in technology, human factors like negligence by customers and employees, fraudulent activity of employees and crackers hackers etc. can become potential source of operational risk. Often there is thin line of difference between operational risk and security risk and both terminologies are used interchangeably.

2.5.2 Security Risk: [34]

Internet is a public network of computers which facilitates flow of data / information and to which there is unrestricted access. Banks using this medium for financial transactions must, therefore, have proper technology and systems in place to build a secured environment for such transactions.

Security risk arises on account of unauthorized access to a bank's critical information stores like accounting system, risk management system, portfolio management system, etc. A breach of security could result in direct financial loss to the bank. For example, hackers operating via the Internet, could access, retrieve and use confidential customer information and also can implant virus. This may result in loss of data, theft of or tampering with customer information, disabling of a significant portion of bank's internal computer system thus denying service, cost of repairing these etc. Other related risks are loss of reputation, infringing customers' privacy and its legal implications etc.

Thus, access control is of paramount importance. Controlling access to banks' system has become more complex in the Internet environment which is a public domain and attempts at unauthorized access could emanate from any source and from anywhere in the world with or without criminal intent. Attackers could be hackers, unscrupulous vendors, disgruntled employees or even pure thrill seekers. Also, in a networked environment the security is limited to its weakest link. It is therefore, necessary that banks critically assess all interrelated systems and have access control measures in place in each of them.

In addition to external attacks banks are exposed to security risk from internal sources e.g. employee fraud. Employees being familiar with different systems and their weaknesses become potential security threats in a loosely controlled environment. They can manage to acquire the authentication data in order to access the customer accounts causing losses to the bank.

Unless specifically protected, all data / information transfer over the Internet can be monitored or read by unauthorized persons. There are programs such as 'sniffers' which can be set up at web servers or other critical locations to collect data like account numbers, passwords, account and credit card numbers. Data privacy and confidentiality issues are relevant even when data is not being transferred over the net. Data residing in web servers or even banks' internal systems are susceptible to corruption if not properly isolated through firewalls from Internet.

The risk of data alteration, intentionally or unintentionally, but unauthorized is real in a networked environment, both when data is being transmitted or stored. Proper access control and technological tools to ensure data integrity is of utmost importance to banks. Another important aspect is whether the systems are in place to quickly detect any such alteration and set the alert.

Identity of the person making a request for a service or a transaction as a customer is crucial to legal validity of a transaction and is a source of risk to a bank. A computer connected to Internet is identified by its IP (Internet Protocol) address. There are methods available to masquerade one computer as another, commonly known as 'IP Spoofing'. Likewise user identity can be misrepresented. Hence, authentication control is an essential security step in any e-banking system. Non-repudiation involves creating a proof of communication between two parties, say the bank and its customer, which neither can deny later. Banks' system must be technologically equipped to handle these aspects which are potential sources of risk.

2.5.3 System Architecture and Design: [35]

Appropriate system architecture and control is an important factor in managing various kinds of operational and security risks. Banks face the risk of wrong choice of technology, improper system design and inadequate control processes. For example, if access to a system is based on only an IP address, any user can gain access by masquerading as a legitimate user by spoofing IP address of a genuine user. Numerous protocols are used for communication across Internet. Each protocol is designed for specific types of data transfer. A system allowing communication with all protocols, say HTTP (Hyper Text Transfer Protocol), FTP (File Transfer Protocol), telnet etc. is more prone to attack than one designed to permit say, only HTTP.

Choice of appropriate technology is a potential risk banks face. Technology which is outdated, not scalable or not proven could land the bank in investment loss, a vulnerable system and inefficient service with attendant operational and security risks and also risk of loss of business.

Many banks rely on outside service providers to implement, operate and maintain their e-banking systems. Although this may be necessary when banks do not have the requisite expertise, it adds to the operational risk. The service provider gains access to all critical business information and technical systems of the bank, thus making the system vulnerable. In such a scenario, the choice of vendor, the contractual arrangement for providing the service etc., become critical components of banks' security. Bank should educate its own staff and over dependencies on these vendors should be avoided as far as possible.

Not updating bank's system in keeping with the rapidly changing technology, increases operational risk because it leaves holes in the security system of the bank. Also, staff may fail to understand fully the nature of new technology employed.

Further, if updating is left entirely at customers' end, it may not be updated as required by the bank. Thus education of the staff as well as users plays an important role to avoid operational risk.

2.5.4 Reputational Risk: [36]

Reputational risk is the risk of getting significant negative public opinion, which may result in a critical loss of funding or customers. Such risks arise from actions which cause major loss of the public confidence in the banks' ability to perform critical functions or impair bank-customer relationship. It may be due to banks' own action or due to third party action.

The main reasons for this risk may be system or product not working to the expectations of the customers, significant system deficiencies, significant security breach (both due to internal and external attack), inadequate information to customers about product use and problem resolution procedures, significant problems with communication networks that impair customers' access to their funds or account information especially if there are no alternative means of account access. Such situation may cause customer-discontinuing use of product or the service. Directly affected customers may leave the bank and others may follow if the problem is publicized.

Other reasons include losses to similar institution offering same type of services causing customer to view other banks also with suspicion, targeted attacks on a bank like hacker spreading inaccurate information about bank products, a virus disturbing bank's system causing system and data integrity problems etc.

Possible measures to avoid this risk are to test the system before implementation, backup facilities, contingency plans including plans to address customer problems during system disruptions, deploying virus checking, deployment of ethical hackers for plugging the loopholes and other security measures.

It is significant not only for a single bank but also for the system as a whole. Under extreme circumstances, such a situation might lead to systemic disruptions in the banking system as a whole. Thus the role of the regulator becomes even more important as not even a single bank can be allowed to fail.

2.5.5 Legal Risk: [37]

Legal risk arises from violation of, or non-conformance with laws, rules, regulations, or prescribed practices, or when the legal rights and obligations of parties to a transaction are not well established. Given the relatively new nature of Internet banking, rights and obligations in some cases are uncertain and applicability of laws and rules is uncertain or ambiguous, thus causing legal risk.

Other reasons for legal risks are uncertainty about the validity of some agreements formed via electronic media and law regarding customer disclosures and privacy protection. A customer, inadequately informed about his rights and obligations, may not take proper precautions in using Internet banking products or services, leading to disputed transactions, unwanted suits against the bank or other regulatory sanctions.

In the enthusiasm of enhancing customer service, bank may link their Internet site to other sites also. This may cause legal risk. Further, a hacker may use the linked site to defraud a bank customer.

If banks are allowed to play a role in authentication of systems such as acting as a Certification Authority, it will bring additional risks. A digital certificate is intended to ensure that a given signature is, in fact, generated by a given signer. Because of this, the certifying bank may become liable for the financial losses incurred by the party relying on the digital certificate.

2.5.6 Money Laundering Risk:

As Internet banking transactions are conducted remotely banks may find it difficult to apply traditional method for detecting and preventing undesirable criminal activities. Application of money laundering rules may also be inappropriate for some forms of electronic payments. Thus banks expose themselves to the money laundering risk. This may result in legal sanctions for non-compliance with "know your customer" laws.

To avoid this, banks need to design proper customer identification and screening techniques, develop audit trails, conduct periodic compliance reviews, frame policies and procedures to spot and report suspicious activities in Internet transactions.

2.5.7 Cross Border Risks:

Internet banking is based on technology that, by its very nature, is designed to extend the geographic reach of banks and customers. Such market expansion can extend beyond national borders. This causes various risks.

It includes legal and regulatory risks, as there may be uncertainty about legal requirements in some countries and jurisdiction ambiguities with respect to the responsibilities of different national authorities. Such considerations may expose banks to legal risks associated with non-compliance of different national laws and regulations, including consumer protection laws, record-keeping and reporting requirements, privacy rules and money laundering laws.

If a bank uses a service provider located in another country, it will be more difficult to monitor it thus, causing operational risk. Also, the foreign-based service provider or foreign participants in Internet banking are sources of country risk to the extent that foreign parties become unable to fulfill their obligations due to economic, social or political factors.

Cross border transaction accentuates credit risk, since it is difficult to appraise an application for a loan from a customer in another country compared to a customer from a familiar customer base. Banks accepting foreign currencies in payment for electronic money may be subjected to market risk because of movements in foreign exchange rates.

2.5.8 Strategic Risk:

This risk is associated with the introduction of a new product or service. Degree of this risk depends upon how well the institution has addressed the various issues related to development of a business plan, availability of sufficient resources to support this plan, credibility of the vendor (if outsourced) and level of the technology used in comparison to the available technology etc. For reducing such risk, banks need to conduct proper survey, consult experts from various fields, establish achievable goals and monitor performance. Also they need to analyze the availability and cost of additional resources, provision of adequate supporting staff, proper training of staff and adequate insurance coverage. Due diligence needs to be observed in selection of vendors, audit of their performance and establishing alternative arrangements for possible inability of a vendor to fulfill its obligation . Besides this, periodic evaluations of new technologies and appropriate consideration for the costs of technological Upgradation are required.

2.5.9 Other Risks: [38]

Traditional banking risks such as credit risk, liquidity risk, interest rate risk and market risk are also present in Internet banking. These risks get intensified due to the very nature of Internet banking on account of use of electronic channels as well as absence of geographical limits. However, their practical consequences may be of a different magnitude for banks and supervisors than operational, reputational and legal risks. This may be particularly true for banks that engage in a variety of banking activities, as compared to banks or bank subsidiaries that specialize in Internet banking.

Credit risk is the risk that a counter party will not settle an obligation for full value, either when due or at any time thereafter. Banks may not be able to properly evaluate the credit worthiness of the customer while extending credit through remote banking procedures, which could enhance the credit risk. Presently, banks generally deal with more familiar customer base. Facility of electronic bill payment in Internet banking may cause credit risk if a third party intermediary fails to carry out its obligations with respect to payment. Proper evaluation of the creditworthiness of a customer and audit of lending process are a must to avoid such risk. Another facility of Internet banking is electronic money. It brings various types of risks associated with it. If a bank purchases e-money from an issuer in order to resell it to a customer, it exposes itself to credit risk in the event of the issuer defaulting on its obligation to redeem electronic money.

Liquidity Risk arises out of a bank's inability to meet its obligations when they become due without incurring unacceptable losses, even though the bank may ultimately be able to meet its obligations. It is important for a bank engaged in electronic money transfer activities that it ensures that funds are adequate to cover redemption and settlement demands at any particular time. Failure to do so, besides exposing the bank to liquidity risk, may even give rise to legal action and reputational risk. Similarly banks dealing in electronic money face interest rate risk because of adverse movements in interest rates causing decrease in the value of assets relative to outstanding electronic money liabilities. Banks also face market risk because of losses in on-and-off balance sheet positions arising out of movements in market prices including foreign exchange rates. Banks accepting foreign currency in payment for electronic money are subject to this type of risk.

Risk of unfair competition: Internet banking is going to intensify the competition among various banks. The open nature of Internet may induce a few banks to use unfair practices to take advantage over rivals. Any leaks at network connection or operating system etc., may allow them to interfere in a rival bank's system.

Thus one can find that along with the benefits, Internet banking carries various risks for bank itself as well as banking system as a whole. The rapid pace of technological innovation is likely to keep changing the nature and scope of risks banks face. These risks must be balanced against the benefits. Supervisory and regulatory authorities are required to develop methods for identifying new risks, assessing risks, managing risks and controlling risk exposure. But authorities need to keep in consideration that the development and use of Internet banking are still in their early stages, and policies that hamper useful innovation and experimentation should be avoided. Thus authorities need to encourage banks to develop a risk management process rigorous and comprehensive enough to deal with known risks and flexible enough to accommodate changes in the type and intensity of the risks.

2.6 Technology and Security Standards for Internet Banking: [39]

The Internet has provided a new and inexpensive channel for banks to reach out to their customers. It allows customers to access banks' facilities round the clock and 7 days a week. It also allows customers to access these facilities from remote sites/home etc. However, all these capabilities come with a price. The highly unregulated Internet provides a less than secure environment for the banks to interface. The diversity in computer, communication and software technologies used by the banks vastly increases the challenges facing the online bankers. In this chapter, an effort has been made to give an overview of the technologies commonly used in Internet banking. An attempt has been made to describe concepts, techniques and technologies related to privacy and security including the physical security. The banks planning to offer Internet banking should have explicit policies on security. An outline for a possible framework for security policy and planning has also been given. Finally, recommendations have been made for ensuring security in Internet banking.

2.6.1 Technologies: Computer Networking & Internet:

The purpose of computer networking is sharing of computing resources and data across the whole organization and the outside world. Computer Networks can be primarily divided into two categories based on speed of data transfers and geographical reach. A Local area network (LAN) connects many servers and workstations within a small geographical area, such as a floor or a building. Some of the common LAN technologies are 10 MB Ethernet, 100 MB Ethernet, 1GB Ethernet, Fiber Distributed Data Interface (FDDI) and Asynchronous Transfer Mode (ATM). The data transfer rates here are very high. They commonly use broadcast mode of data transfer.

The Wide Area Network (WAN), on the other hand, is designed to carry data over great distances and are generally point-to-point. Connectivity in WAN set-up is provided by using dial-up modems on the Public Switched Telephone Network (PSTN) or leased lines, VSAT networks, an Integrated Services Digital Network (ISDN) or T1 lines, Frame Relay/X.25 (Permanent Virtual Circuits), Synchronous Optical Network (SONET), or by using Virtual Private Networks (VPN) which are software-defined dedicated and customized services used to carry traffic over the Internet. The different topologies, technologies and data communication protocols have different implications on safety and security of services.

To standardize on communications between systems, the International Organization of Standards developed the OSI model (the Open System Interconnection Reference Model) in 1977. The OSI breaks up the communication process into 7 layers and describe the functions and interfaces of each layer. The important services provided by some of the layers are mentioned below. It is necessary to have a good understanding of these layers for developing applications and for deploying firewalls (described later).

- **Application Layer:** Network Management, File Transfer Protocol, Information validation, Application-level access security checking.
- **Session Layer:** establishing, managing and terminating connections (sessions) between applications.
- **Transport Layer:** Reliable transparent transfer of data between end points, end to end recovery & flow control.
- **Network Layer:** Routing, switching, traffic monitoring and congestion control, control of network connections, logical channels and data flow.
- **Data Link Layer:** Reliable transfer of data across physical link and control of flow of data from one machine to another.

Protocols:

The data transmission protocol suite used for the Internet is known as the Transmission Control Protocol/Internet Protocol (TCP/IP). The Internet is primarily a network of networks. The networks in a particular geographical area are connected into a large regional network. The regional networks are connected via a high speed "back bone". The data sent from one region to another is first transmitted to a Network Access Point (NAP) and are then routed over the backbone. Each computer connected to the Internet is given a unique IP address (such as 142.16.111.84) and a hierarchical domain name(such as cse.iitb.ernet.in).The Internet can be accessed using various application-level protocols such as FTP (File Transfer Protocol), Telnet (Remote Terminal Control Protocol), Simple Mail Transport Protocol (SMTP), Hypertext Transfer Protocol (HTTP). These protocols run on top of TCP/IP. The most innovative part of the Internet is the World Wide Web (WWW). The web uses hyperlinks, which allow users to move from any place on the web to any other place. The web consists of web pages, which are multimedia pages composed of text, graphics, sound and video. The web pages are made using Hypertext Markup Language (HTML). The web works on a client-server model in which the client software, known as the browser, runs on the local machine and the server software, called the web server, runs on a possibly remote machine. Some of the popular browsers are Microsoft Internet Explorer and Netscape Navigator. With the popularity of web, organizations find it beneficial to provide access to their services through the Internet to its employees and the public. In a typical situation, a component of the application runs (as an 'applet') within the browser on user's workstation. The applet connects to the application (directly using TCP/IP or through web server using HTTP protocols) on the organization's application and database servers. These servers may be on different computer systems. The web-based applications provide flexible access from anywhere using the familiar browsers that support graphics and multimedia. The solutions are also scalable and easy to extend.

Banking Products:

Internet Banking applications run on diverse platforms, operating systems and use different architectures. The product may support centralized (bankwide) operations or branch level automation. It may have a distributed, client server or three tier architecture based on a file system or a DBMS package. Moreover, the product may run on computer systems of various types ranging from PCs, open (Unix based) systems, to proprietary main frames. These products allow different levels of access to the customers and different range of facilities. The products accessible through Internet can be classified into three types based on the levels of access granted:

Information only systems:

General-purpose information like interest rates, branch locations, product features, FAQs, loan and deposit calculators are provided on the bank's web (WWW) site.

The sites also allow downloading of application forms. Interactivity is limited to a simple form of 'e-mail'. No identification or authentication of customers is done and there is no interaction between the bank's production system (where current data of accounts are kept and transactions are processed) and the customer.

Electronic Information Transfer System:

These systems provide customer specific information in the form of account balances, transaction details, statement of account etc. The information is still largely 'read only'. Identification and authentication of customer takes place using relatively simple techniques (like passwords). Information is fetched from the Bank's production system in either the batch mode or offline. Thus, the bank's main application system is not directly accessed.

Fully Transactional System:

These systems provide bi-directional transaction capabilities. The bank allows customers to submit transactions on its systems and these directly update customer accounts. Therefore, security & control system need to be strongest here.

2.6.2 Application Architecture:

A computer-based application may be built as a monolithic software, or may be structured to run on a client-server environment, or even have three or multi-tiered architecture. A computer application typically separates its 3 main tasks: interactions with the user, processing of transactions as per the business rules, and the storage of business data. The three tasks can be viewed as three layers, which may run on the same system (possibly a large, proprietary computer system), or may be separated on to multiple computers (across the Internet), leading to three-tier or multi-tier architecture. These layers can be briefly described as follows:

Presentation Layer :

This layer is responsible for managing the front-end devices, which include browsers on personal computers, Personal Digital Assistants (PDAs), mobile phones, Internet kiosks, Web TV etc. The presentation layer takes care of user interface related issues like display details, colour, layout, image etc. It also has important responsibilities in user authentication and session management activity.

Application layer :

It contains the business logic (for processing of data and transactions) and necessary interfaces to the data layer. It processes requests from the presentation layer, connects to the data layer, receives and processes the information and passes results back to the presentation layer. It is responsible for ensuring that all the business rules are incorporated in the software. The issues of scalability, reliability and performance of the services to a great extent depend upon the application layer architecture.

Data Layer :

The data layer uses a database package to store, retrieve and update application data. The database may be maintained on one or multiple servers. A database package also supports back-up and recovery of data, as well as logging of all transactions.

2.6.3 Issues in Administration of Systems and Applications: [40]

The role of the network and the database administrator is pivotal in securing the information systems of any organization. The role extends across various job functions and any laxity in any of the functions leaves the system open for malicious purposes. A few important functions of the administrator and how they relate to or impinge on system security are discussed below:

Installation of Software:

A software (whether system or application) needs to be carefully installed as per the developer's instructions. The software system may contain bugs and security holes, which over a period are fixed through appropriate patches. It is necessary to know the latest and correct configuration of all software packages. Hackers and intruders are often aware of these bugs and may exploit known weaknesses in the software; hence, care should be taken to install only the latest versions of software with the latest patches. Further, improper installation may lead to degradation of services. Installation of pirated software is not only illegal and unethical, but may also contain trojans and viruses, which may compromise system security. In the case of installation of outsourced software, care should be taken to compare the source code and the executable code using appropriate tools as unscrupulous developers may leave backdoor traps in the software and for illegal access and update to the data. In addition, while installing software care should be taken that only necessary services are enabled on a need to use basis.

Access Controls and User Maintenance :

An administrator has to create user accounts on different computer systems, and give various access permissions to the users. Setting access controls to files, objects and devices reduces intentional and unintentional security breaches. A bank's system policy should specify access privileges and controls for the information stored on the computers. The administrators create needed user groups and assign users to the appropriate groups. The execution privilege of most system-related utilities should be limited to system administrators so that users may be prevented from making system level changes. The write / modify access permissions for all executables and binary files should be disabled. If possible, all log files should be made "append only". All sensitive data should be made more secure by using encryption. The system and database administrators are also responsible for the maintenance of users and the deletion of inactive users. Proper logs should be maintained of dates of user creation and validity period of users. There should be a frequent review to identify unnecessary users and privileges, especially of temporary users such as system maintenance personnel and system auditors.

Backup, Recovery & Business Continuity :

Back-up of data, documentation and software is an important function of the administrators. Both data and software should be backed up periodically. The frequency of back up should depend on the recovery needs of the application. Online / real time systems require frequent backups within a day. The back-up may be incremental or complete. Automating the back up procedures is preferred to obviate operator errors and missed back-ups. Recovery and business continuity measures, based on criticality of the systems, should be in place and a documented plan with the organization and assignment of responsibilities of the key decision making personnel should exist. An off-site back up is necessary for recovery from major failures / disasters to ensure business continuity. Depending on criticality, different technologies based on back up, hot sites, warm sites or cold sites should be available for business continuity. The business continuity plan should be frequently tested.

System & Network Logging :

Operating systems, database packages and even business applications produce a 'log' of various tasks performed by them. Most operating systems keep a log of all user actions. Log files are the primary record of suspicious behavior. Log files alert the administrator to carry out further investigation in case of suspicious activity and help in determining the extent of intrusion. Log files can also provide evidence in case of legal proceedings. The administrator has to select types of information to be logged, the mechanisms for logging, locations for logging, and locations where the log files are stored. The information required to be logged should include Login/Logout information, location and time of failed attempts, changes in status,

status of any resource, changes in system status such as shutdowns, initializations and restart; file accesses, change to file access control lists, mail logs, modem logs, network access logs, web server logs, etc. The log files must be protected and archived regularly and securely.

2.6.4 Security and Privacy Issues: Terminology: [41]

Security:
Security in Internet banking comprises both the computer and communication security. The aim of computer security is to preserve computing resources against abuse and unauthorized use, and to protect data from accidental and deliberate damage, disclosure and modification. The communication security aims to protect data during the transmission in computer network and distributed system.

Authentication:
It is a process of verifying claimed identity of an individual user, machine, software component or any other entity. For example, an IP Address identifies a computer system on the Internet, much like a phone number identifies a telephone. It may be to ensure that unauthorized users do not enter, or for verifying the sources from where the data are received. It is important because it ensures authorization and accountability. Authorization means control over the activity of user, whereas accountability allows us to trace uniquely the action to a specific user. Authentication can be based on password or network address or on cryptographic techniques.

Access Control:
It is a mechanism to control the access to the system and its facilities by a given user up to the extent necessary to perform his job function. It provides for the protection of the system resources against unauthorized access. An access control mechanism uses the authenticated identities of principals and the information about these

principals to determine and enforce access rights. It goes hand in hand with authentication. In establishing a link between a bank's internal network and the Internet, we may create a number of additional access points into the internal operational system. In this situation, unauthorized access attempts might be initiated from anywhere. Unauthorized access causes destruction, alterations, theft of data or funds, compromising data confidentiality, denial of service etc. Access control may be of discretionary and mandatory types.

Data Confidentiality:

The concept of providing for protection of data from unauthorized disclosure is called data confidentiality. Due to the open nature of Internet, unless otherwise protected, all data transfer can be monitored or read by others. Although it is difficult to monitor a transmission at random, because of numerous paths available, special programs such as "Sniffers", set up at an opportune location like Web server, can collect vital information. This may include credit card number, deposits, loans or password etc. Confidentiality extends beyond data transfer and include any connected data storage system including network storage systems. Password and other access control methods help in ensuring data confidentiality.

Data Integrity:

It ensures that information cannot be modified in unexpected way. Loss of data integrity could result from human error, intentional tampering, or even catastrophic events. Failure to protect the correctness of data may render data useless, or worse, dangerous. Efforts must be made to ensure the accuracy and soundness of data at all times. Access control, encryption and digital signatures are the methods to ensure data integrity.

Non-Repudiation:

Non-Repudiation involves creating proof of the origin or delivery of data to protect the sender against false denial by the recipient that data has been received or to protect the recipient against false denial by the sender that the data has been sent. To ensure that a transaction is enforceable, steps must be taken to prohibit parties from disputing the validity of, or refusing to acknowledge, legitimate communication or transaction.

Security Audit Trail:

A security audit refers to an independent review and examination of system's records and activities, in order to test for adequacy of system controls. It ensures compliance with established policy and operational procedures, to detect breaches in security, and to recommend any indicated changes in the control, policy and procedures. Audit Trail refers to data generated by the system, which facilitates a security audit at a future date.

2.6.5 Attacks and Compromises: [42]

When a bank's system is connected to the Internet, an attack could originate at any time from anywhere. Some acceptable level of security must be established before business on the Internet can be reliably conducted. An attack could be any form like:

- The intruder may gain unauthorized access and nothing more.
- The intruder gains access and destroys, corrupt or otherwise alters data
- The intruder gains access and seizes control partly or wholly, perhaps denying access to privileged users
- The intruder does not gain access, but instead forges messages from your system
- The intruder does not gain access, but instead implements malicious procedures that cause the network to fail, reboot, and hang.

Modern security techniques have made cracking very difficult but not impossible. Further more, if the system is not configured properly or the updated patches are not installed then hackers may crack the system using security hole. A wide range of information regarding security hole and their fixes is freely available on the Internet. System administrator should keep himself updated with this information. Common cracking attacks include:

- E-mail bomb and List linking
- Denial-of-Service
- Sniffer attack
- Utilizing security hole in the system software
- *E-mail bomb:* This is a harassment tool. A traditional e-mail bomb is simply a series of message (perhaps thousands) sent to your mailbox. The attacker's object is to fill the mailbox with junk.
- *Denial-of-Service (DoS) attacks:* DoS attacks can temporarily incapacitate the entire network(or at least those hosts that rely on TCP/IP). DoS attacks strike at the heart of IP implementations. Hence they can crop up at any platform, a single DoS attack may well work on several target operating systems._Many DoS attacks are well known and well documented. Available fixes must be applied.
- *Sniffer Attack*: Sniffers are devices that capture network packets. They are a combination of hardware and software. Sniffers work by placing the network interface into promiscuous mode. Under normal circumstances, all machines on the network can "hear" the traffic passing through, but will only respond to data addressed specifically to it. Nevertheless, if the machine is in promiscuous mode then it can capture all packets and frames on the network. Sniffers can capture passwords and other confidential information. Sniffers are extremely difficult to detect because they are passive

programs. Encrypted session provides a good solution for this. If an attacker sniffs encrypted data, it will be useless to him. However, not all applications have integrated encryption support.

- *Holes:* A hole is any defect in hardware, software or policy that allows attackers to gain unauthorized access to your system. The network tools that can have holes are Routers, Client and Server software, Operating Systems and Firewalls.

2.6.6 Authentication Techniques: [43]

As mentioned earlier, authentication is a process to verify the claimed identity. There are various techniques available for authentication. Password is the most extensively used method. Most of the financial institutions use passwords along with PIN (Personal Identification Number) for authentication. Technologies such as tokens, smart cards and biometrics can be used to strengthen the security structure by requiring the user to possess something physical.

Token technology relies on a separate physical device, which is retained by an individual, to verify the user's identity. The token resembles a small hand-held card or calculator and is used to generate passwords. The device is usually synchronized with security software in the host computer such as an internal clock or an identical time based mathematical algorithm. Tokens are well suited for one-time password generation and access control. A separate PIN is typically required to activate the token.

Smart cards resemble credit cards or other traditional magnetic stripe cards, but contain an embedded computer chip. The chip includes a processor, operating system, and both Read Only Memory (ROM) and Random Access Memory (RAM). They can be used to generate one-time passwords when prompted by a host computer, or to carry cryptographic keys. A smart card reader is required for their use.

Biometrics involves identification and verification of an individual based on some physical -characteristic, such as fingerprint analysis, hand geometry, or retina scanning. This technology is advancing rapidly, and offers an alternative means to authenticate a user.

2.6.7 Firewalls: [44]

The connection between internal networks and the outside world must be watched and monitored carefully by a gatekeeper of sorts. Firewalls do this job. Otherwise, there is a risk of exposing the internal network and systems, often leaving them vulnerable and compromising the integrity and privacy of data. Firewalls are a component or set of components that restrict access between a protected network and the outside world (i.e., the Internet). They control traffic between outside and inside a network, providing a single entry point where access control and auditing can be imposed. All firewalls examine the pieces or packets of data flowing into and out of a network and determine whether a particular person should be given access inside the network. As a result, unauthorized computers outside the firewall are prevented from directly accessing the computers inside the internal network. Broadly, there are three types of firewalls i.e. Packet filtering firewalls, Proxy servers and tasteful inspection firewall. Packet filtering routers are the simplest form of firewalls.

The bastion host directs message accepted by the router to the appropriate application servers in the protected network. Their function is to route data of a network and to allow only certain types of data into the network by checking the type of data and its source and destination address. If the router determines that the data is sourced from an Internet address which is not on its acceptable or trusted sources list, the connection would be simply refused. The advantage of this type of firewall is that it is simple and cheaper to implement and also fast and transparent to the users. The disadvantage is that if the security of the router were compromised, computers on the internal network would be open to external network for attacks. Also, the filtering rules can be difficult to configure, and a poorly configured firewall could result in security loopholes by unintentionally allowing access to an internal network. Proxy servers control incoming and outgoing traffic for a network by executing specific proxy program for each requested connection. If any computer outside the internal network wants to access some application running on a computer inside the internal network, then it would actually communicate with the proxy server, and proxy server in turn will pass the request to the internal computer and get the response which will be given to the recipient (outside user). That is, there is no direct connection between the internal network and Internet. This approach allows a high level of control and in-depth monitoring using logging and auditing tools. However, since it doubles the amount of processing, this approach may lead to some degradation in performance. Fig. 3 shows a typical firewall organization consisting of 'militarized zone' that separates the protected network from the Internet.

Stateful Inspection firewall:

This type of firewalls thoroughly inspects all packets of information at the network level as in the case of proxy servers. Specifications of each packet of data, such as the user and the transportation method, the application used are all queried and verified in the inspection process. The information collected is maintained so that all future transmissions are inspected and compared to past transmission. If both the "state" of the transmission and the "context" in which it is used deviate from normal patterns, the connection would be refused. This type of firewalls are very powerful but performance would also decline due to the intensive inspection and verification performed.

Cryptography: [45]

The process of disguising a message in such a way as to hide its substance is called encryption. An encrypted message is called cipher text. The process of turning a cipher text back into plain text is called decryption. Cryptography is the art and science of keeping messages secure. It uses a 'key' for encrypting or decrypting a message. Both the method of encryption and the size of key are important to ensure confidentiality of a message. There are two types of encryption: Symmetric key and Asymmetric key encryption. In the symmetric key cryptography scheme, the same key is used to encrypt and decrypt the message. Common symmetric algorithms include One-time pad encryption, Data Encryption Standard (DES), Triple DES, LOKI, Twofish, Blowfish, International Data Encryption Algorithm (IDEA). DES and Triple DES are the commonly used techniques. Asymmetric key cryptography scheme is also known as Public key crypto-system. Here two keys are used. One key is kept secret and therefore it is referred as "private key". The other key is made widely available to anyone who wants it, and is referred as "Public key". The Public key and Private key are mathematically related so that information encrypted using the public key can only be decrypted by the corresponding private key and vice-versa. Importantly, it is near to impossible to find out the private key from the public key. Common and more popular public key cryptosystem algorithms are Diffie-Hellman, RSA, Elliptic Curve etc. In all these, the confidentiality is directly related to the key size. Larger the key size, the longer it takes to break the encrypted message.

- ❖ *Diffie-Hellman*: This is the first public key algorithm invented. It gets its security from the difficulty of calculating discrete logarithms in a finite field. Diffie-Hellman method can be used for distribution of keys to be used for symmetric encryption.
- ❖ *RSA:* Named after its three inventors, Ron Rivest, Adi Shamir and Leonard Adleman, who first introduced the algorithm in 1978, RSA gets its security from the difficulty of factoring large numbers.

The public and private keys are function of a pair of large (100 or 200 digits or even larger) prime numbers. The pair is used for asymmetric encryption.

2.6.8 Digital Signature and Certification: [46]

Digital signatures authenticate the identity of a sender, through the private, cryptographic key. In addition, every digital signature is different because it is derived from the content of the message itself. The combination of identity authentication and singularly unique signatures results in a transmission that can not be-repudiated.

Digital signature can be applied to any data transmission, including e-mail. To generate digital signature, the original, unencrypted message is processed through mathematical algorithms that generate a 'message digest' (a unique character representation of data). This process is known as "hashing". The message digest is then encrypted with the private key and sent along with the message (could be encrypted also). The recipient receives both the message and encrypted message digest. The recipient decrypts the message digest using the sender's public key, and then runs the message through the hash function again. If the resulting message digest matches the one sent with the message, the message has not been altered and data integrity is verified. Because the message digest was encrypted using the private key, the sender can be identified and bound to the specific message.

2.6.9 Certification Authorities and Digital Certificates: [47]

Certificate Authorities and Digital Certificates are emerging to further address the issues of authentication, non-repudiation, data privacy and cryptographic key management. A Certificate Authority (CA) is a trusted third party that verifies the identity of a party to a transaction. To do this, the CA vouches for the identity of a party by attaching the CA's digital signature to any messages, public keys, etc., which are transmitted. The CA must be trusted by the parties involved, and identities must have been proven to the CA beforehand. Digital certificates are messages that are signed with the CA's private key. They identify the CA, the represented party, and even include the represented party's public key.

Secure Socket Layer (SSL): [48]

SSL is designed to make use of TCP to provide a reliable end-to-end secure service. The SSL servers have digital certificates issued by Certifying Authorities so that the clients can authenticate the service provider (a bank in our case). The servers use a password /PIN/digital certificate to authenticate clients. Once the clients and server have authenticated each other, they establish a session key for encryption of messages. The diagram above shows flow of messages in SSL. The flow of authentication messages in SSL is shown in Fig.6.4.

Public Key Infrastructure (PKI): [49]

Public key cryptography can play an important role in providing needed security services including confidentiality, authentication, digital signatures and integrity. Public key cryptography uses two electronic keys: a public key and a private key. The public key can be known by anyone while the private key is kept secret by its owner. As long as there is strong binding between the owner and the owner's public key, the identity of the originator of a message can be traced to the owner of the private key. A Public Key Infrastructure (PKI) provides the means to bind public keys to their owners and helps in the distribution of reliable public keys in large heterogeneous networks. Public keys are bound to their owners by public key certificates. These certificates contain information such as the owner's name and the associated public key and are issued by a reliable Certification Authority (CA).

PKI consists of the following components:[50]

- *Key Certificate* - An electronic record that binds a public key to the identity of the owner of a public-private key pair and is signed by a trusted entity.
- *Certification Authority (CA)* - A trusted entity that issues and revokes public key certificates
- *Registration Authority (RA)* - An entity that is trusted by the CA to register or vouch for the identity of users to the CA.
- *Certificate Repository* - An electronic site that holds certificates and CRLs. CAs post certificates and CRLs to repositories.
- *Certificate Revocation List (CRL)* - A list of certificates that have been revoked. The list is usually signed by the same entity that issued the certificates. Certificates can be revoked for several reasons. For example, a certificate can be revoked if the owner's private key has been lost or if the owner's name changes.
- *Certificate User* - An entity that uses certificates to know, with certainty, the public key of another entity.

The widespread use of PKI technology to support digital signatures can help increase confidence of electronic transactions. For example, the use of a digital signature allows a seller to prove that goods or services were requested by a buyer and therefore demand payment. The use of a PKI allows parties without prior knowledge of each other to engage in verifiable transactions.

Confidentiality and PKI: A PKI could also support confidentiality services using a public-private key pair that is different from the one used for signing. In this case, users need to obtain a separate certificate for the confidentiality public key. To send an encrypted message, a user could obtain the recipient's confidentiality certificate from a certificate repository and verify that it is valid. Then the sender can encrypt the message using the public key. Only the recipient, in possession of the private key, will be able to decrypt the message.

Certificates: Although there have been several proposed formats for public key certificates, most certificates available today are based on an international standard (ITU-T X.509 version 3). This standard defines a certificate structure that includes several optional extensions. The use of X.509v3 certificates is important because it provides interoperability between PKI components. Also, the standard's defined extensions offer flexibility to support specific business needs.

PKI Architectures:
A PKI is often composed of many CAs linked by trust paths. The CAs may be linked in several ways. They may be arranged hierarchically under a "root CA" that issues certificates to subordinate CAs. The CAs can also be arranged independently in a network. Recipients of a signed message with no relationship with the CA that issued the certificate for the sender of the message can still validate the sender's certificate by finding a path between their CA and the one that issued the sender's certificate. The National Institute of Standards and Technology (NIST) has developed a hybrid architecture specification based on both a hierarchical and a network architecture model in the document, Public Key Infrastructure (PKI) Technical Specifications (Version2.3): Part C - Concept of Operations.

2.6.10 Physical Security: [51]

Physical security is a vital part of any security plan and is fundamental to all security efforts--without it, information security, software security, user access security, and network security are considerably more difficult, if not impossible, to initiate. Physical security is achieved predominantly by controlled and restricted physical access to the systems resources. *Access control* broadly provides the ability to grant selective access to certain people at certain times and deny access to all others at all times. Physical security involves the protection of building sites and equipment (and all information and software contained therein) from theft, vandalism, natural disaster, manmade catastrophes and accidental damage (e.g., from electrical surges, extreme temperatures and spilled coffee). It requires solid building construction, suitable emergency preparedness, reliable power supplies, adequate climate control, and appropriate protection from intruders. Thus, in broad terms, the focus is on restricting access to the computer area, controlling access to all vulnerable and sensitive areas of the department, and monitoring of all staff and visitors.

Physical Access can be secured through the following means: Bolting Door locks and Combination Locks, Electronic Door Locks, Biometric Door Locks, Manual Logging, Electronic Logging, Photo Identification Badges, Video Cameras stationed at strategic points, Controlled Visitor Access. A bank should also have in place environmental controls to manage exposures from fire, natural disasters, power failure, air-conditioning failure, water damage, bomb threat / attack etc. A few means of obtaining control over environmental exposure are:

- The server room and any other unattended equipment room should have water detector. Fire extinguishers should be placed at all strategic points, supplementing fire suppression systems with smoke detectors, use of fire resistant materials in office materials including furniture, redundant power supply from two substations, electrical wiring placed in fire resistant panels and conduits and documented and tested evacuation plans.
- It is important to educate all 'stake-holders' (users, employees, etc) about the importance of physical security. This education should be carried out as part of 'social engineering'.

Security Policy:

The information security policy is the systemization of approaches and policies related to the formulation of information security measures to be employed within the organization to assure security of information and information systems owned by it. The security policy should address the following items:

- Basic approach to information security measures.
- The information and information systems that must be protected, and the reasons for such protection.
- Priorities of information and information systems that must be protected.
- Involvement and responsibility of management and establishment of an information security coordination division.
- Checks by legal department and compliance with laws / regulations.
- The use of outside consultants.
- Identification of information security risks and their management.
- Impact of security policies on quality of service to the customers (for example, disabling an account after three unsuccessful logins may result in denial of service when it is done by somebody else mischievously or when restoration takes unduly long time).
- Decision making process of carrying out information security measures.
- Procedures for revising information security measures.
- Responsibilities of each officer and employee and the rules (disciplinary action etc) to be applied in each case.
- Auditing of the compliance to the security policy.
- User awareness and training regarding information security.
- Business continuity Plans.
- Procedures for periodic review of the policy and security measures.

The top management of the bank must express a commitment to security by manifestly approving and supporting formal security awareness and training. This may require special management level training. Security awareness will teach people not to disclose sensitive information such as password file names. Security guidelines, policies and procedures affect the entire organization and as such, should have the support and suggestions of end users, executive management, security administration, IS personnel and legal counsel.