CHAPTER I
INTRODUCTION

1.1 EVOLUTION PROCESS OF BANKING

Many evolutions have taken place in the growth and development of banking sector. There cannot be any one unique response to the question of definition of banking. This is because bank is not a single action performer. Bank performs not only numerous functions but also variety of services which are impossible to be covered under one individual definition. An ordinary man perceives bank as a means of saving and withdrawing money and a businessman perceives it as an organization for lending finance. In short, banking refers to anything and everything that a bank does. But this short explanation is not sufficient to understand the term “Banking” in detail. One of the famous dictionaries interprets as a set up for safety of liquid cash which in turn is paid to the customers depending upon their expectation. But even this interpretation is incomplete within itself as it covers only deposit and repayment aspect of banking, as mentioned in the beginning. The subject of banking has its own roots followed by the stages of growth and development. Therefore it is time to discuss about bank’s evolution. The roots of term “Bank” can be understood as follows:

- Banck as a word in the German language which means joint stock fund. (from here it moved to the next step i.e.)
- Banca a word in the Italian language which means mountain of money. (after this next step was)
- Bancus or Banque a word in the French language which implies a desk where valuables can be safeguarded. (ultimately comes)
- The word Bank in the English language which refers to an organization which renders service of depositing cash for the purpose of financing or withdrawal.
Reserve bank of India is considered as a banker’s bank that governs and regulates all the banks under the banking regulation act (1949). Banking means the functions of accepting the deposits from public and availing withdrawal of cash via withdrawal slips, cheques, automated teller machine etc. therefore, it is assumed that these functions of accepting and withdrawal of money must not be performed by any organisation without prior permission of bankers bank i.e. reserve bank of India. The functions, on evolution of the modern banks can be traced at the important roots i.e. first one is the goldsmith, next comes is the moneylender, followed by the merchant bankers. Being a dealer of gold which is an extremely valuable thing, goldsmith possesses all the facilities for safeguarding. Therefore, he accepted public money which is another extremely valuable thing. Not only this, once he realized that public will not ask for return of their money at the same time, he started lending it at a good rate of interest. Likewise, moneylenders also helped poor people by making them available his surplus cash at affordable rate of interest. Next in the sequence comes is the merchant bankers who are traders and help people by accepting their funds as a safeguard. Thus, the qualities of these three individuals i.e. goldsmith, moneylender and merchant banks are possessed by a modern bank today. After imposition of strict rules and regulations by the king Charles private banks slowly took the place of goldsmiths.

Evolution of banking system in India:

Indian banking system is as ancient as Himalayas. But the tasks or functions to be performed by the banks were highlighted only after twentieth century. History of Indian banking was initiated due to the efforts taken by East India Company. There are many authors who have defined bank. Some of them are Crowther, Hant.L, Kinley, Paget, John and Sayers. According to all of them banking is an institution, organization or a set up which avails the facility of accepting the money from those who have it in surplus or they have saved it from their income. Then after accepting it bank allows them to withdraw by cheque or otherwise lend to those who require it. This way bank utilizes the money of those who do not require it by giving it to those who require it at a reasonable interest rate thereby creating income for the bank. It utilizes the funds accepted either
for repaying, lending or investments. Banks are not only protectors of funds but also producers of funds.

**Characteristics of modern system of banking:**

- **Dealers of deposits:** banks allow people to deposit their surplus fund with them and lend these funds to the needy people. These deposits accepted by the banks can be current, fixed, savings or recurring. People have to comply with different terms and conditions associated with these deposit schemes.

- **Withdrawal of deposits:** banks allow public to withdraw their deposits by using cheques, withdrawal slip or draft or pay order. This function is performed by the banks only on demand.

- **Dealers in credit:** banks not only safeguard the funds but also create additional funds. They do it by earning interest. Thus, they are manufacturer of credit. Therefore, “creation of funds” is additional characteristic of banks.

- **Profit motive:** banking is purely a commercial set up since all the functions are performed by the bank with profit motive.

- **Principle of agent:** besides being an acceptor of funds and lending it as a loan, bank is also known as an agent due to its numerous services of agency kind.

**Significance of Indian private sector banks:**

Although Indian economy consists of public and private sector banks, private banks play an important role in the economy of India. They promote growth of public sector banks indirectly by giving them a vigorous competition. Some of the important features of private banks have been listed down as follows:
• **Creating healthy atmosphere and competition:** private sector banks not only promote healthy atmosphere but also healthy competition, on the administration levels in the banking infrastructure as well as banking operation systems.

• **Highly efficient and professional management:** the work culture of private sector banks is well equipped with highly professional administrative. Besides this, modern concepts of marketing are also introduced in the banking system. Doing this, they also promote public sector banks to grow with similar kind of efficiency and technology.

• **Promotes international investment:** international investment within the economy is highly influenced by the foreign banks which come under the purview of private sector banks.

• **Easy approach to international capital markets:** government agencies and companies of Indian economy get assistance from foreign private sector banks for fulfilling their financial requirements from foreign capital markets. Existence of one of the branch or head office of foreign banks in well known foreign countries makes this access all the more easier for our country. Besides promoting international investment, private sector banks also promote growth of trade and industries within the economy.

• **Innovative development and achieve specialization:** marketing of innovative products and services to the customers as well as industries is a kind of habit of private sector banks. They help the industries to attain specialization in their fields by availing those services of higher quality. Not only this, they also introduce novelty of technology in the banking sector.

### 1.2 ELECTRONIC BANKING AND INTERNET BANKING

Banks have become a part and parcel of all economic activities in India. A bank is an institution which deals in money and credit. Thus, bank is an intermediary which handles other people’s money both, for their advantage and to its own profit. But bank is not merely a trader in money but also an important manufacturer of pool of services
related to money may it be withdrawal, deposit or lending of money in various forms and through various means. Execution of all these services for the ease and comfort of the customers to fulfill their needs is known as BANKING.

Process of banking provides a platform to the people to come across banks and complete their all requirements related to funds or money.

But with growing competition within the economy and lack of sufficient time in hand people started finding it difficult to visit banks any time, howsoever urgent it may be for them. Sometimes the need of funds may arise on Sundays and public holidays. It is difficult for the people to access to the banks on such days. Therefore, need of the hour was that if there could be some technique which could meet financial needs of the people even during non-banking hours from their own account balances. Since need is the mother of invention, E-BANKING i.e. ELECTRONIC BANKING came into existence which is through electronic channels. Many understand E-banking as Internet banking which is incorrect. E-Banking is electronic banking which has a wider horizon and it includes many electronic facilities such as ATMS i.e. automated teller machines, debit cards, credit cards, smart cards and many others. Amongst these one of the most popular and important E-banking service is INTERNET BANKING. Thus internet banking is one of the components of electronic banking.

The term E-banking or electronic banking is an innovative way of doing banking transactions. Banks find electronic banking as a powerful ‘value added’ tool to attract and retain new customers along with additional benefit by avoiding costly paper handling and teller interactions in rapidly growing competitive banking environment. Electronic banking is like a wider sea which includes the following droplets within it:

1. **ATM (Automated Teller Machine):** Indian economy has witnessed evolutions one amongst which is related to money. Evolutions have taken place from cash money to
cheque money and then plastic card which is witnessed with the discovery of ATMS. ATM performs one of the most important functions of the banks. It is made up of plastic card which replaces cheque, Personal presence of the customer, banking hour’s limitation and paper work. ATM provides facilities like withdrawal of cash, deposit of cash or cheque, balance enquiry, mini statement, mobile recharging and fund transfers etc. Customers are given a unique identification number for executing the transactions from these ATMS. External appearance of ATM i.e. Automated Teller Machine seems to be like that of a weighing machine meant for humans installed on the railway stations. But there are certain differences too. Weighing machines weigh the weight of a living being in kilogram where automated teller machine observes the balance of a human in terms of rupees. The process of measuring weight in weighing machine involves two steps i.e. inserting a coin and then rekeying a card with weight and future written on it. But in case of automated teller machine it is not so, it involves inserting or swapping of a plastic card and then receiving cash and bank balance receipt etc. Does it mean on insertion of just a plastic card everyone receives cash? Is it a magic? To know this we must study in detail, how does automated teller machine functions?

**Operational working of ATM card:**
Those customers who are having savings account and currents account with the banks with certain amount of minimum balance are provided with an automated teller machine card. Moment user inserts the card in the automated teller machine, identification is done by machine’s censor hardware and then user is asked to enter one’s identification i.e. PIN. This code number is allotted to each and every customer by the bank. Therefore, bank staff also knows this number. User identifies oneself by pressing buttons installed on the automated teller machine. In turn, automated teller machine immediately cross examines the account number of user on the card with the help of a secret code number which is inside the automated teller machine. If both the numbers tally, automated teller machine gives various options to the user asking his requirements. User can chose anything from the menu which is displayed on the screen. It may be cash withdrawal, balance enquiry, mini statement, change of pin code etc. Each option on the menu has sub options for example if user selects withdrawals---
amount in multiples etc. After entering all the details paper currency notes are thrown out of the machine. This denomination of money is immediately debited to the users account. Each and every bank prefers to restrict the maximum limit of money that an individual can withdraw from the automated teller machine. This facility is offered to the account holders 24*7. Personal identification number is the biggest protection against misutilisation of automated teller machine debit card. ATM facility was primarily offered by HSBC bank in the year 1987. Currently there are numerous banks availing ATM facility in urban as well as in the rural areas. It provides comfortability and secrecy of transactions via self service. There are several advantages of using ATM some of them are written as follows:

- This service is available at any point of time irrespective of season or night duration. Besides, it does not require recruitment of any employee by the bank;
- Automated teller machine debit card is an alternative availability to those who are not having credit card for meeting their financial requirements whenever they need;
- Customers do not need to visit the branch where their accounts are maintained, provided automated teller machines are installed and networked efficiently;
- It offers mechanical and immediate accounting.
- Installation of CCTV surveillance may reduce the probability of fraud.

2. **Debit Card**: a card which is issued by the banks having access to one’s bank account directly is referred to as Debit card. It is termed as debit card because the moment customer swipes debit card, amount is immediately debited to his bank account. It is a card issued by the banks which allows its owner to utilise funds for the payment of purchases. It is a type of prepaid card with already certain stored value. Each time a customer uses this card the electronic banking department transfers the money to a particular account from the account of the customer and the customer’s account is debited with exact amount of purchases. The customer has to open an account with the bank which issues debit card along with personal identification number (PIN). When he purchases something he enters his pin number on that shop’s pin pad. The moment card is slurped through electronic terminal it connects to the related bank system which
validates the pin and confirms from the concerned bank whether to accept or reject the
payment. No chances of overspending because system does not accept the amount
more than the balance in the account. Like credit card here no credit facility along with
credit period is provided to the customers and therefore, criteria of minimum income
level are not needed for usage of debit card. Debit card basically has combined features
of an ATM card as well as cheque. Before usage of debit card it is the responsibility of
the user to maintain sufficient balance in the account. Debit card is cost effective as
compared to credit card. It is like using our own money with the help of electronic
channels.

3. Credit Card: It is a kind of post paid card which empowers its owner to spend wherever
and whenever one wants within the limits fixed by his bank. The credit card holder is
granted credit of 25 to 50 days to pay in case there are insufficient funds in the account
at the time of spending. However, a credit card holder is charged with a service fee for
this facility offered to him.

Operational working process of credit card is described in the following sequences:

- On application and filling the form, user receives the credit card;
- All the procedures, formalities and arrangements are completed amongst the user and
  the banking authority and the seller;
- User uses credit card for payment of purchases and puts his initials on the bills;
- Shopkeeper in turn sends all the bills and details to the concerned bank;
- The concerned bank then makes all the payments to the seller;
- The user is intimated about these purchases by the bank;
- On due date or thereafter user makes the payment to the bank.

Positive aspects of credit card:

Following are some of the benefits of the credit card to the bank as well as the user and
the seller:

- This mode of payment helps the banks to attract more and more customers;
- Usage of credit card by the customers gives an opportunity to the banks to gain profit
  from the sales turnover of the seller or the shopkeeper;
• Users satisfaction is enhanced due to availability of additional and easy service given by the bank;
• Maximum usage of credit card by the customer results into additional turnover which in turn is good for country’s economical growth and for increased banking habits amongst people;
• Huge network of credit card users implies positive image and better popularity of the banks;
• Those expenses which are incurred to administer clearing operations will be reduced to a great extent for example expenses on printing and stationery, (manpower) i.e. peons and clerks;
• If user of credit card facility takes loan from the bank for settlement of credit bills, it increases bank’s income by way of additional interest;
• Risk of credit card is reduced for the bankers because banks issue credit cards to the customer only after screening their financial position.

4. Smart Card: Smart card looks exactly like an ATM card with additional feature of integrated circuit(IC chip) installation. This is done for higher security and more reliability reasons. Smart cards have bright future in banking sector because they store a huge amount of information about their owners like medical and health history.

5. Mobile Banking: Mobile Banking takes place when financial transactions are completed by logging into the website of the bank using a mobile phone. These financial transactions may include viewing and checking account balances, intra fund transfers and payment of bills. Mobile banking is a phrase used for performing financial transactions via a mobile device such as a mobile phone. It is often executed via sms.

6. Telephone Banking: Through telephone banking, banks and financial institutions provide a service which enables customer to transact their financial transactions over the telephone without necessity of physical banking. Many financial institutions offer this service on 24*7 basis. From view point of banks, it is a cost reducing service because it reduces the customer’s need to visit the banks personally except for cash withdrawals
and deposit transactions. It is an informative kind of service. To avail telephone banking service, a customer is supposed to register with the bank and a secret code identification number is given to the customer exactly like in usage of automated teller machine card. Maximum banks providing telephone banking services use an automated phone answering system with voice identification capability. In case, a customer needs to enquire about one's own bank balance or some other information is required relating to bank account, phone number given by the bank is dialled up. After this dialling an automated recorded voice identifies a user with the help of a secret code number as well as account number. Upon tallying of number, all the required information is given to the user on the telephone. For security reasons it is must for a customer to first authenticate through a password or by responding to security questions interrogated by a live representative.

7. Internet Banking: banking is a service motive activity. One of the ways in which service is provided to the customers is through computer network. Online banking is nothing but extended mode of banking services with the help of automated computer network. Since the invention of IT banks have been in forefront of using technology to improve their marketing share. Over a long period of time they have been using electronic and telecommunication channels for delivering a large range of value added products and services. With the popularity of easy access to internet and World Wide Web (WWW) banks initiated using internet as a network for receiving instructions and selling their products and services to the customers. This kind of banking is known as internet banking. Although the products and services offered through internet banking by different banks differ. The Reserve Bank of India has constituted a working group on internet banking. The group has divided the internet banking in India broadly into three types on the basis of levels of access granted. These three types are as follows:

A: Information only system: It is a basic level service available in the banks websites which provides information on variety of products and services offered by the banks to their customers and the public. At this level various types of application forms can be downloaded. Queries of customers are received and replied through e-mails. No
interaction takes place between the banks’ system and the customers, therefore even identification of customers’ is not required. At this level it is not possible for any unauthorised person to get into channel and system of the bank via internet.

**B: Electronic Information Transfer System:** Also known a simple transactional websites that enable customers to input their instructions or queries for account balances and ask for statement of their accounts. Still, the information is mainly of the ‘Read only’ mode. Recognition of the customer is done through password. At this level customers are not permitted to perform any fund based transactions through their accounts.

**C: Fully Electronic Transactional System:** At this level fully transactional websites of the banks enable customers to perform upon all the services as offered in physical banking like transfer of funds, various payments, buying and selling of securities etc. At this level highest degree of security, privacy and control is expected. (Abha Singh 2012)

In this way, comprising of all the above three levels together different banks provide different facilities and services to their customers through internet banking but the most common and popular ones are as follows:

1. Balance Inquiry and Mini Statement of Account
2. Apply for Issue of Cheque Book
3. Viewing of Account Information
4. RTGS/NEFT Transactions
5. Status Inquiry of Outward Cheques
6. Electronic payment of Direct Taxes, Indirect Taxes, etc.
7. Apply for Term Deposit and Fixed Deposits
8. Managing the Payment of Credit Card
9. Detailed information of Holding / Statement of Demat Accounts
10. Loan EMI Inquiry
11. Enquiry about Types of Loans
12. Pension and Investment patterns
13. Bill Payment Service
14. Railway Pass (Indian railways tie up with ICICI Bank)
15. Recharging Prepaid Phone
16. Shopping online provided tie up with shopping websites. (B. N. Kapoor 2009)

Payments can be made with the help of internet banking via RTGS and NEFT. It means nothing but they are different modes of payment. Short form for NEFT is National Electronic Fund Transfer. Under this mode of payment a service is given to the users in which one can transfer the funds from any branch of the concerned bank to other branch of any bank, both within the same city as well as outside the city. Requests send by the users for neft dealings are executed on the same day by the bank only if they are accessed prior to four p.m. on working days from Monday upto Friday. If it is weekend i.e. Saturday then request is executed if it is applied prior to twelve p.m.

Short form for RTGS is Real Time Gross Settlement. Using this mode of payment introduced by Banker’s Bank, an individual can transfer the funds in real span of time. The receiver of the funds gets the amount within time limit of two hours. Requests sent by the users for RTGS transactions are processed by the banks on the same day only if they are received prior to two p.m. on working days i.e. from Monday to Friday. If it is weekend i.e. Saturday then it must be received prior to Eleven o’clock in the morning for execution. This mode of payment is basically used by the customers for transactions involving huge amount. RTGS can be utilised for transactions involving transfer of minimum one lakh cash.

Positive aspects of internet banking:

The positive impacts of internet banking are very obvious. Business and corporate class consumers look into their savings as well as business account information. Besides, cutting down on a trip to the bank, one can check the account balance whenever needed irrespective of banking working hours. This is not enough; one can make payment of bill on line, thereby saving both money and time on postal service. One of
the advantages of online banking is the possibility of easily comparing the services availed by different online banks. One can purchase financial products online and at the same time can also apply for various types of loans. While doing so comparison can be made between the various options given by different banks to assure that best possible option is selected. One can even inspect insurance policies with the help of armchair banking. Financial securities and investments like stocks and bonds can be conveniently managed with net banking sitting at home or from workplace without depending on a financial mediator like stock broker.

Negative aspects of internet banking:

Certain issues which are seeking attention as a negative impact of internet banking have been:

- **Loss of jobs and increasing levels of employment:** there is no visible employment loss in the banking sector because of huge expansion. Certain foreign banks have also witnessed expansion by increasing their number of branches and operational area. Infact as per (Economic Times, 1992) twelve banks were given permission in January 1992 to open forty four additional branches in different cities of Indian economy. However, a reduction has been noticed in the recruitment rate of nationalised banks. Expansion of new technology may result in labour savings. The developments like recognition of voice, recognition of optical character will definitely replace labours. A tendency may develop on the part of higher authorities to discontinue bargaining staff. This is because computerisation of administrative job reduces the requirement of physical administrators.

- **Increased workloads:** innovative techniques may reduce the repetitive work of some operations but the number of operations on the other hand may increase for example a cashier was supposed to record thirty to forty cash entries on a single day previously in pre computerisation period but in post computerisation period being with computers he is supposed to enter hundred cash entries. Work pressure has increased with more work load. Automation of work along with non recruitment and no
appointment in place of retired staff has resulted into increased workload. On completion of twenty years of job, staff is bound to be exhausted and fed up which in turn will be tagged as unfit or old age by the management.

- **Pressure of being flexible**: management always insists on flexibility so as to be able to respond immediately to operational changes taking place in the growing market. Management always argues that flexibility is must to deal with innovations in technology, to manage fluctuating patterns in the work flow. All these requirements can be fulfilled only by employing a multi-skilled employee. They don’t prefer to appoint several persons specialised in several fields. Innovations in technology expect recruitment of multi-functioning employees instead of specialised ones.

- **Alterations in job profile**: changes in the work assigned have its own positive as well as negative implications. Although efficiency in terms of productivity has increased, now staff hardly gets time to communicate with each other. They again need to concentrate and train themselves on the new work assigned to them. Communication with customers is more after computerisation but the work has become stressful for the employees.

- **Insecurity feeling**: due to automation contractual staff is appointed for specific work without intimating to the employee. Any reduction on job framework always scares the staff and creates insecurity within them. Those who are not highly trained for computer operations always work with the feeling of insecurity. Sometimes employees are asked to take VRS i.e. forced retirement before the due period.

- **Deteriorating conditions of health and safety**: emergence of technology has welcomed a set of new problems along with developments. The production of new hardware and materials, systems and processes in the market with inadequate information of their post usage effect may create problems in the future. Certain health problems are very common due to continuous sitting in front of the computer hardware. Although computerisation of banking administration is a thing of past, certain manual
works were carried out by staff which gave them a good break from computer screen. But since introduction of internet banking, sitting work in front of computer is unending. Staffs suffer from various health problems such as infections in eyes, masculine pain, headaches and also problems related to reproduction like miscarriages. Staff works right from 9 a.m. in the morning upto 5 p.m. in the evening and sometimes even more than that. Hardly fifteen or twenty minutes break is given in between for lunch and tea. Inspite of giving extensive training to the staff for computers health issues are never mentioned. Although there is wide information available on health issues related to continuous working on computer, employees ignore it. Lack of awareness on the part of employees and lack of concern on the part of management may create serious health problems in our nation in the near future.

1.3 DIFFERENCE BETWEEN ELECTRONIC-BANKING, INTERNET BANKING, TELEPHONE BANKING AND MOBILE BANKING

E-Banking i.e. electronic banking is a broader in spectrum which encompasses of ATM cards for withdrawal of cash or making the payment with credit card even without visiting the bank or without going online. Any banking transaction done through electronic channels comes under E-banking which includes internet banking, mobile banking and telephone banking under its shadow. That simply implies no need to visit banks physically still you communicate your needs to the bank either through telephone or mobile or via internet connection.

In telephone banking you communicate with your bank by dialling a special telephone number and a code number to which bank responds via automated system through speech recognition and DTMF technology or may be via live customer service representatives. In telephone banking you request banking officer to do the needful or you get the thing done from them rather than performing over those transactions at your own like in internet banking and mobile banking, Whereas in internet banking you
perform the transaction at your own by authenticating your identity through a unique password. In internet banking you have to visit to the bank’s website, choose for internet banking, login your password and then proceed further for your requirements. It may be with wire or without wire i.e. through your PC or through your mobile. However mobile banking is always wireless which enables you to do transactions through your smart phone using bank’s mobile banking software such as sbi freedom. Nowadays banks download this application on your mobile device free of charge. After downloading this software you can anytime perform mobile banking. You just need to open that software and gates of bank are opened for you to transact directly in your account without the need to go to Google and then search for the bank’s website like in internet banking.

1.4 INTERNET BANKING IN FOREIGN COUNTRIES

- **Scandinavia**: Finnish banks and Swedish banks are the leading banks in the world in terms of quality of internet banking services offered by them. All over the world Sweden bank is the first bank to initiate with EBPP. It is referred as electronic bill presentation and payment. Till 2011 payment of almost two million bills were handled. They are using advanced level of encryption technology. Adoption of an efficient system referred to as Challenge Response Logic is an additional feature of Scandinavian banks. In this system each and every internet banking customer is sent a list of code number by the banks. Every customer is supposed to use these code numbers in sequences along with their PIN or personal identification number. Thus, usage of this system provides every banking transaction, a unique and secret code which till now has proved to be safe. Certain banks are efficient enough to use sophisticated version of this system.

Besides, complying with national laws every European country is required to follow directives issued by European Union. Data protection directives all over Europe are passed by European Union. Aim of these directives was to provide better protection to the users against misutilisation of their confidential and personal information. Even telecommunication directives have been passed by the union of Europe which provide protected techniques in terms of cell phone communications, digital television etc.
Implementation of European Union directives in terms of electronic sign is mandatory too in national laws.

- **New Zealand**: amongst various banks offering net banking services to the customers, maximum banks operate their net banking services as a section of the bank instead of an individual legal body. Same approach is followed by Reserve bank in New Zealand for smooth operations of online banking transactions as well as traditional banking transactions. However, there are certain regulations for supervision which are applicable only for online banking.

- **Australia**: in the country Australia net banking is offered in two modes: one with the help of proprietary software and another one is web based. Novice web based products and services concentrated on personal banking whereas proprietary software was used for corporate sector and business firms. Maximum banks in Australia and their foreign subsidiaries as well, have websites of interactive mode. In Australia EBPP i.e. electronically bill payment and presentment is still at its early stage. Facilities which are offered to corporate sectors and business firms with the help of proprietary software include account report, payroll functionality, and edited reconciliation and inter or intra bank account fund transfers. These services are offered either via dial-up or extranet feature.

- **Singapore**: MAS which is also referred as Monetary Authority of Singapore has an authority of licensing banks to prove its relevance in the field of online banking developments. These existing banks can begin with a separate entity or a specialised department for internet banking. Even new competitors entering the banking sector can initiate with “Internet Bank Only” identity. Flexibility is given to the banks to decide upon whether net banking will be started in a subsidiary bank or within the same existing bank for which further licensing is not necessary. Risk association with internet banking is well known to everyone. A supervisory strategy based on risk of individual bank’s scenario and situation is given significant importance by monetary authority of Singapore rather than a regulation as such “one-size-fits-all”. Each bank is supposed
to disclose its risk management approach to monetary authority of Singapore. In this risk management strategy every bank must (i) execute proper workflow, process of authentication and control system surrounding access system; (ii) plan and execute disaster management plans and policies; (iii) appoint a professional and specialist to examine its security system; (iv) give accurate and clear information to the customers in terms of rights as well as responsibilities not only of the customers but also of the banking institution itself, especially in the case of incidents arising due to mistakes in security system of banks. Continuous encouragement is shown by monetary authority of Singapore for financial institutions and Singapore association of banks to educate customers on online banking.

**Hongkong:** the monetary authority of Hongkong makes it compulsory for every bank that it must elaborate risk management plans and policies prior of introducing a transactional website. This authority is authorised to inspect security’s systems and get reports either from the internal supervisory or from the external and professional who is appointed to prepare such reports. Monetary authority of hongkong executes its supervision in such a way that discussion is held with individual bank desiring to begin with internet banking. This is not enough. Banks are even allowed to show how efficiently they have installed their security system in following ways:-

(i) Encryption of information accessible by intruders with the help of authorised techniques.

(ii) Measures adopted to avoid unauthorised intrusion into computer system of the bank.

(iii) Developing comprehensive security strategies and technique.

(iv) Reporting of all fraudulent incidents to the monetary authority of hongkong and sufficient securities measures adopted depending upon the need of the hour.

According to the guidelines given by the monetary Authority of honkong (a) it will not take any objection on setup of any internet banking in hongkong provided all compliances have been done with prudential criteria which are applicable to traditional banks also b) an internet bank desiring to perform banking activity in hongkong must
have physical branch also. c) Level of security must be maintained by every virtual bank depending upon the type of banking activities it wishes to execute. While Applying for internet banking submission of report by professional expert on the aspects of hardware security of computer d) Installation of efficient methods and measures of security to handle the risks involved in operations. e) Setting of clear terms and conditions related to provision of its services. f) If guidelines given by the monetary authority of the hongkong on outsourcing are taken care of Virtual bank can even outsource their business to a third party service merchant. Hongkong banks are supposed to assure that the relevant laws are complied with while offering armchair banking services. For safeguarding the interest of customers banking practise code is revised from time to time. Advertisement for acceptance of deposits to a place situated outside Hongkong is an offence. Besides, mutual identification, cross verification of digital signatures should also be done amongst certificate authorities.

• **JAPAN**: Net banking is significant part of Japanian banking strategy. The rule of mandatory physical branch in Japan has witnessed alterations as to consideration of license of banks and those branches which do not have physical existence. Safeguarding of personal information has become a burning aspect in Japanian banks. According to law banks in Japan are recommended to keep disclosure publications at their working place. But it is not easy to fulfil this requisite by “internet only banks”. In Japan no restrictions are imposed on usage of cryptography. However, reporting of this technique is required to be done to international trade and industry ministry.

• **UNITED STATES OF AMERICA**: Dependence on outsider vendors is very common which is observed in the United States. In united it is not necessary for an existing bank to follow up any notification requirement in order to begin with online banking services. However, an advance notice of thirty days is required if bank desire to setup an operational website. In case of internet banking supervisory approach, legal requirements and regulation for licensing are almost similar to that of conventional banking. Whereas, in terms of risks faced by armchair banking, agenises of federal banks have issued not only procedures for examination but also guidelines of
supervision to be followed by those who supervise online banking services. Requirement of security lab is also declared by Technology Secretariat of Banking Industry to examine and authorise the security of banks both the sections i.e. software as well as hardware. If there is a reliance on third party seller then evaluation of such vendor’s operations is required to be done by an additional agency of federal bank to make supervision approach all the more stronger and effective.

**Indian Scenario on internet banking:**

According to Morgan Stanley as compared to any other sector, web is more valuable for banking sector. Toady Indian banks are proceeding with retail banking in much better and effective way as compared to traditional one. Still, there is a long way to go. There are certain factors revealed by scholars of IIML.

- Throughout the Indian economy net banking is at blossoming stage of development.
- International and private banking sector is better developed in respect of website development.

Today scenario is observed by the scholars that the banks who will not offer internet banking will be marginalised. Due to availability of electronically channelized services at reduced cost there is a pressure on the banks. Increased awareness amongst the customers for requirement of transparency, it has now become mandatory for the banks to install the best and highly effective security measures and techniques. Much has to be achieved in the field of educating and training Indian customers for usage of maximum armchair banking facilities.

### 1.5 TYPES OF RISKS

Internet banking has revolutionized the banking industry. However it is associated with a wider array of risks and threats which the banks and other financial institutions are trying to tackle jointly.
Reserve Bank of India has set up a working committee to evaluate and analyze different bottlenecks relating to net banking and suggest technological, legal and operational standards keeping in mind the international practices. Following are some of the risks discussed which serves as the baseline for deciding on general risk control guidelines.

1) **Operational Risk**: it is the most common form of risk associated with net banking. It is also known as transactional risk. It can be in the form of incorrect processing of transactions, failure in data integrity, data privacy and confidentiality, unauthenticated entry to the system and transactions of the bank. Such risks arise due to weaknesses in infrastructure, execution and supervision of information system of bank. Besides technological bottlenecks, ignorance by customers and officials and indulgence of employees and hackers in fraudulent activities can be important reasons for operational risks. Both the terms operational risk and security risk are used for each other due to hair line difference between them.

2) **Security Risk**: internet is a network of computers available to the public for access to unlimited information. For using it for the execution of financial transactions banks must have proper infrastructure and technology to facilitate a well secured environment for customers.

Security risk occurs due to unauthenticated and unidentified intrusion to banks information system, accounting system or risk management system. Failure of security system may lead to financial loss to the banks. Hackers may use internet for unauthorized access and retrieval of customer’s information and can also install a virus. This may lead to undesirable use of customer’s information and obstruction to banks computer infrastructure, denying access and then resulting into cost of restructuring the same. Besides this banks may lose reputation and share of customers market. Intruders could be hackers, dissatisfied employees or simply thrill enjoyers. Therefore, it is must for the banks to evaluate and examine their all intra related systems and establish access controlling measures for better security.
Besides facing external threats banks may also face internal threats from their own employees. Employees are very well versed with banks' security systems as well as their weak points. They may get authenticated data to access customers’ accounts resulting into banks' loss. All the data or information that is transferred through internet can be easily accessed by unauthorized persons unless it is specifically secured. A program named Sniffer can be implanted at web server or other places to retrieve data related to customers' account ID- password, credit card number etc. security of data is a critical issue even if it is not transferred through internet. Information stored in the banks internal infrastructure is also vulnerable to unauthorized access threat if it is not protected from internet by firewalls. In an internet connected environment there are always chances that data may be changed by unauthorized figures may it be willingly or unwillingly. This risk may occur at both the stages either when data is stored or when it is transferred. Set up of efficient technological tools and access control measures are of great importance for the banks. And it is equally important that these are in place to immediately identify such data changes and make the officials alert. An internet connected computer is recognized through its internet protocol (IP) address. Through IP spoofing it is easy to (masquerade) one computer as another. Similarly customers' identity can be misutilised. Therefore account identification and authentication tools are important security measures in internet banking system.

System infrastructure and design: Accurate system infrastructure and efficient control measures is a significant factor in handling different kinds of operational and security risks. Banks experience the risk of incorrect selection of technology. Inadequate system infrastructure and strict control processes. It is not desirable that access to system should be based only on IP address because in such a case anybody can represent himself as a genuine user by spoofing the actual or the real users IP address. Many protocols have been designed for access through internet. Each protocol is for a particular type of data transfer. A system which enables communication or access through every protocol may it be HTTP (hyper text transfer protocol), FTP (file transfer protocol), telnet is more vulnerable to attacks than a system which allows only one protocol say HTTP. Selection of appropriate technology is a significant challenge faced
by the banks. An inappropriate, outdated and inaccurate technology results into financial as well as business loss to the banks. Lack of techno savvy expertise compels banks to depend on outside service providers for execution and supervision of their internet banking system. This may result into operational risk because outsiders gain access to all the technical parts of the system as well as significant information about the bank which makes the system more prone to risk. In these circumstances selection of service provider and their methods for rendering service proves to be of great importance for security of banks. To avoid such risk maximum efforts should be taken by the banks to train its employees. If system of the bank is not updated in keeping pace with new and advent technology operational risk increases along with bottlenecks in the banks system. At the same time the employees may not understand the working of new technology installed. Moreover updating cannot be left completely at customers end because in that case it may not be updated as desired by the banks. Therefore, educating employees along with customers is of great importance to reduce operational risk. Measures that can be taken up to provide security against operational risks are to access control, digital signature, usage of firewalls, cryptographic techniques, public key encryption etc.

3) Reputational Risk: It is a risk of damaging institutions image and building negative opinion amongst minds of people resulting into a heavy loss of customers. Such risk decreases the confidence and trust of public in the banks efficiency to perform any function. Moreover, it spoils the banks relationships with its customers. Chances of such risk increase if the system or product of the bank is not up to the expectations of the customers. Similarly there could be other reasons like major deficiencies in system infrastructure, security violation may it be due to internal or external attacks, insufficient information passed on to the customers regarding product usage, major problem with communication network which prevents access to their account details and funds especially when there is no other alternative way of communications. Under such situation customers may stop using products or services of the banks. Those customers who are directly suffered may close their accounts with bank other customers may also follow the trend if negative points of banks are publicized. Another reason causing
reputational risk could be loss suffered by the similar type of institution rendering services of the same kind. Loss of image of similar type of institution causes customers to build the same opinion about other banks. They build suspicious image of the banks in their minds. Similarly, other reason for reputational risk could be that hackers spread rumors about the products and services of the bank.

Banks should take up maximum measures to avoid reputational risk like before execution system should be tested, there should be back up facilities, emergency plans which should also cover strategy to address problems of the customers, during system interruption installing virus checking, employment of ethical hackers for removing the loopholes of the system.

Positive image and good reputation is important not only for a single bank but for the entire banking system on a macro level. Therefore, the role of controller and regulator becomes all the more important as failure of single bank develops suspicious image about entire banking system at a large.

4) **Legal Risk:** Legal risk arises due to breach of or non-compliance with laws, established practices, rules and regulations or if legal rights and privileges of customers are not taken care of by the banks. If customers are not informed properly about their rights and responsibilities, they may not take adequate precautions in buying products or services through internet banking. Such circumstances may result into undesirable disputed transactions. In order to increase market share of customers sometimes banks connect their internet banking website to other sites which in turn may cause legal risk. Moreover attackers or hackers may use the connected site to cheat any customer of the bank.

5) **Money Laundering Risk:** Since internet banking transactions are rarely conducted it may be difficult for the banks to identify and prevent unexpected fraudulent activities. For certain specific internet payments application of money laundering may not be possible. In order to prevent such kind of risks accurate and adequate user identification techniques, periodic reviews and proper policies and procedures should be framed.
With the help of such measures detection of suspicious transactions in internet banking would be easier.

6) **Cross Border Risks:** Internet banking has basically changed the image of banking system from brick to click. It is designed in such a way to extend its geographical limits. Such extended market share may also reach the height of national borders which in turn may cause various risks. It covers legal as well as regulatory risks because there are differences with respect to legal requirements of different countries jurisdiction, ambiguities about responsibilities of different authorities at national level. In such scenario banks may become vulnerable to risk related to non-compliance with national laws, rules and regulations, consumer protection laws, privacy and security rules and also money laundering laws.

Monitoring and supervision becomes all the more difficult if service providers appointed by the bank resides in the foreign countries. It may also cause operational risk. In case of internet banking, may it be service provider or participating bank if they are foreign based chances of risk are to the extent that overseas parties are not able to fulfill obligations because of political, social and economic factors.

Foreign transactions increase risk of credit lending as it is difficult to consider a loan application from a foreign based customer compared to a customer from inland. Acceptance of foreign currencies as a payment through internet banking may be vulnerable to risk due to changes (variations) in foreign exchange rates.

7) **Strategic Risk:** Launch of innovative product or service is always associated with strategic risk. The percentage of this risk depends upon various factors. These factors include how efficiently banks have studied the various issues related to designing of a business plan, adequacy of resources to accomplish this plan, credit stability of the service provider, advancement in new technology used as compared to the technology already in existence. Banks should avoid such risk through proper survey, consultation with experts, setting attainable aims and supervision of performance. They should also
examine the adequacy and cost structure of new resources, availability of sufficient staff as well as training of staff along with insurance coverage. Besides these enough care should be taken in choice of service provider and availability of alternative in case of failure of service provider to complete its responsibilities. Moreover, in order to upgrade the technology, its periodical evaluation in comparison to cost is also essential.

8) Risk of Unfair Competitions: Increased competitions amongst the banks to enhance their market era of consumers through internet banking may compel certain banks to start unfair practices. Intensified competition may bring them down to such an extent that through any leaks in network or operating system they may interfere with the system of their competitor banks.

1.6 FRAUDS ASSOCIATED WITH INTERNET BANKING

The terms like internet banking crime, electronic crime, digital crime are used as synonyms in net banking. Some of the common frauds associated with net banking are as follows:

- **Phishing**: phishing includes spoofing. It is nothing but mimicking of an authenticated website or email to lure the user in a net and make him believe that it is an original one. This is done to retrieve personal information from the users like banking account details, credit card number, password etc. Normally, the URL of spoofed website is similar to that of legitimate one. The originality in the duplicate website is created by copying the graphics or bank’s logo from the original website. Proper path is followed by the fraudsters i.e. primarily retrieving the personal information of the user and then using it for withdrawals of cash from user’s account.
- **ID theft** is one kind of phishing fraud.
• **Jacking of website**: it takes a forceful control on the bank’s website by an individual. The actual financial institution loses its control on appearance of the website.

• **Worm**: as name indicates, it is a virus with different breed. One of them can be of destructive nature, another one which seems to safeguard one’s computer from viruses but actually bring virus into the computer system. The most risky is of the kind in which it gets installed into your computer system while accessing some sites or WebPages and then it observes and captures keystrokes of the users and sends them to the fraudsters sitting in another corner of the computer. Once again it is a different way followed to steal personal information of the user. One of the biggest examples of worm is bugbear family. It is a massive form of worms which is targeted on to the financial institutions. It spreads within the entire network of computer system. Bugbear also has the capability to defunct the bank’s antivirus software.

• **Spyware**: spyware is a tool used by the criminals to steal customer’s information from internet connection without the knowledge of customers. There can be variety of spywares like harmless advertisements in the form of pop-ups. Thus, it could be an ability that records everything from the user’s computer and then sends it to the culprit. It looks like Trojan horse or worm but it is difficult to differentiate.

• **Denial of service**: it is aimed at harming the user by bringing a halt to the computer network. Generally, the target is server. Typically, net banking servers through which access is provided to the online transactions and data. Distributed denial of service is a higher version of denial of service in which through user’s computer numerous attacks are targeted simultaneously flooding the server of financial institutions and making it disabled.

• **Hacking**: it is also termed as cracking. In lucid language it is nothing but an unauthorized intrusion into the computer network and stealing customer’s personal information. It is done by writing or using readymade program to attack a computer.

1.7 **RECOMMENDATIONS GIVEN BY THE RBI COMMITTEE**
Each coin has its two sides. Every new technology comes with its own advantages as well as disadvantages. Similarly, even internet banking along with the benefits carries various types of risks for banks at micro level and whole banking system at macro level. The nature and scope of risks faced by the banks, change with levels of technological advancement. But authorities should set up tools and methods for detecting risks, evaluating risks, handling risks and most important for controlling these risks.

E- Banking is the innovative way of selling traditional banking products and services to the customers through electronic channels. These services are accessed by the customers using a personal computer, ATM, internet, Debit card or credit card.

Being the highest authority RBI had appointed an internet banking Committee. This committee had examined different aspects of internet banking and concentrated on major areas of net banking i.e.

- Technology and Security areas
- Legal areas and
- Regulatory and supervisory areas

On the basis of recommendations of committee many guidelines have been given to the banks for implementation. Following are those guidelines:

**Technology and Security Areas**

- Every bank must appoint a network and database officer with clearly defined duties as stated in the committee report.
- Each bank must have its own security policy which is approved by Board of directors. Similarly, there should be clear division of duties between security officers i.e. one who concentrates only on security of information system and IT division which implements
the entire computer system. Besides this an auditor should be appointed to audit the information system.

- In order to safeguard the data system application, system software and communication lines logical access control measures should be introduced by banks. These measures may be in the form of user- ids, passwords or physical or behavioral biometric technologies.

- In order to avoid direct connection between the bank’s system and internet and to have higher level of control and better monitoring banks should use the proxy server type of firewall. Even past and present transactions are compared. It includes a real time security alert.

- Similarly, usage of 128-bit SSL secured Socket Layer is recommended to ensure authenticity of server and use of client certificate which are issued by the banks themselves with the help of certificate server.

- Usage of 128- bit SSL for security of browser to web serve communication and encryption of passwords in transit.

- Similarly, application server should be segregated from the E-mail server.

- Any kind of computer access should be logged. Security attacks should be kept in mind and considered while framing the future security policies. Against these intrusions and attacks latest tools, monitoring systems and networks should be acquired by the banks. At the same time banks should evaluate and examine their security measures and policies in the light of their own experiences. Security personnel as well as customers should be educated and trained on regular basis.

- Every bank must have proper infrastructure for backing up of data and it should be properly tested before using.

- Security officer as well as security auditor of the banks should test the system periodically in the following ways:-

  - They should try to guess passwords with the help of password cracking tools;
  - Tests may also be conducted by appointing external experts (Ethical hackers).

Legal Areas
Looking at the prevalent crimes in the banking sector although banks encourage more and more customers to use internet banking, requests for opening a new account should be accepted by the banks only after accurate introduction, verification and authentication of the identity of the applicants. This authentication procedure followed by the banks as a security measure must be approved by the Law.

As a moral responsibility and ethics point of view it is must that every bank should maintain complete secrecy and confidentiality about details of customer. But it is very difficult in today’s internet banking scenario due to several factors. Inspite of many precautions banks are highly vulnerable to attackers and hackers. Therefore, banks should install accurate and adequate risk control tools and measures to avoid such intrusions. All banks should clearly explain their customers’ timeframe and situations under which STOP PAYMENT instruction would be accepted.

In India the rights of consumers defined by the Consumer Protection Act 1986 are applicable to banking services also. In present scenario the rights and responsibilities of internet banking users are determined by bilateral agreements between the bankers and the customers. However, it is of utmost importance that banks must insure themselves against risks like unauthorized transfer.

**Regulatory and Supervisory Areas**

According to the recommendations made by the committee the current framework of rules and regulations of banks will be applied to online banking too. Therefore,

a) Only those banks which are supervised and licensed in India and whose physical infrastructure is situated in India are allowed to offer internet banking services to Indian residents. Thus the banks which are registered outside the country and do not have any physical infrastructure within the country will not be allowed to provide internet banking to Indian customers.

b) Similarly, products should be made available to account holders only.
c) The services rendered should promote only local current products.
d) Indian banks will not be allowed to offer internet banking services to the customers in other border jurisdiction. Similarly, banks in existence in other border jurisdiction will not be allowed to offer internet banking service to the Indians customers.
e) Banks who desire to offer internet banking services at transactional level are supposed to seek prior permission from RBI and application for such permission must state its business plans, cost structure, technology adopted and system and control measures to avoid risks. Similarly, security policy stating recommendations and a certificate from an auditor certifying that minimum requirements have been met with should be enclosed. Once permission approved any significant changes in the services of products should be intimated by the banks to RBI.
f) Banks are supposed to inform RBI about each and every failure of security tools and measures and in turn RBI at its will may ask the special audit and supervision of such banks.
g) Banks must decide upon guidelines to handle the risks arising due to third party service providers such as defective service and officers of service providers getting intimate knowledge about banks system and misutilising the same.
h) Due to increased usage of E-commerce it is necessary to decide upon interbank payment gateways for settlement of e-commerce transactions. Similarly, rules and regulations for such payments gateways must be followed as per directions given by the committee.
i) Only member banks of cheque clearing system will be allowed to be a part of interbank payment gateway for settlement of internet banking payments. Transactions arising due to usage of credit cards, overseas e-commerce dealings and intra bank payment will not be allowed to be settled through interbank payment gateways.
j) All interbank payment gateways should be capable to deal with NEFT as well as RTGS transactions within stipulated period of time.
k) Link between the payment gateway and computer infrastructure of member bank should be established with the help of a leased line network (i.e. without internet) as per encryption standard. Besides, authentication of every transaction must be digitally certified by reputed licensed agency of certification. Before the customer's access RBI
may check the security of entire system at payment gateways front and the institutions
front.

l) Bilateral contracts between the receiving bank and paying bank and service provider will
serve as the legal proof for such payments. The privileges and responsibilities of each
party should be clearly notified to be valid in the eyes of law.

m) It should be mandatory for each and every bank to publish their latest financial results.
Similarly, each bank should compulsorily disclose the risks, duties and obligations of the
customers using internet banking.

n) Hyperlinks related to the websites of the bank may influence the goodwill of the bank. It
may cause reputational risk. Hyperlinks through banks websites should further be
connected only to those areas or sites which give information related to product or
services purchased by bank’s customers. It should not present such image of the bank
that any irrelevant or any product or service not related to banking is advertised by the
banks. It should be mandatory for all the banks to follow security precautions while
handling customers purchase related requests from other websites.

It is decided by Reserve Bank of India that committee's recommendations should be
followed by every bank providing internet banking services. And although
recommendations have been given for online banking they should be adopted for all
forms of electronic banking to the extent of their relevancy.

In order to see strict adherence with recommendations banks providing net banking
services are suggested to review their system and submit the report to RBI. This report
should clearly cover the different types of services, extent of their follow up with
recommendations, non compliance and their future plans indicating the time limit for
follow up.

Physical security: although generally, this aspect of security is overlooked by banking
authorities, it is necessary that physical access controlling measures and techniques
should be seriously and sincerely adhered to. Physical security must include the entire
information system and the place where computer network system is installed. It should be under strict supervision against both interior and exterior threatening walls.

Physical security is an important aspect of any security plan and it is a basic concern of all the types of security efforts. Physical security in true sense of the word can be attained only by controlling and restricting physical access to the resources of a computer network system. Appropriate emergency measures, uninterrupted electricity supply, suitable and controlled temperature, climatic control and strict protection from unauthorized intrusion is must. Thus, in short concentration should be on prohibiting the access to network of computers and supervision of employees and visitors. Following are some of the tips which can be followed to secure physical access:

- Provision of combination of locks;
- Provision of automated locks for the doors;
- Provision of door lock which require biometric for authentication;
- CCTV surveillance at sensitive areas;
- Banking infrastructure should also cover installation of appropriate changing environment metal detectors to administer fire exposure, damage due to water, failure of air conditioner. For this it should be taken care that all sensitive areas not only have fire extinguishers but also smoke and water detectors;
- Furniture which is used to accommodate commuter network should be fire resistant;
- Likewise, electric wiring should be fit in the panels and coverings which are fire resistant;
- Similarly to handle emergency situations, evacuation plans should be demonstrated and tested.

1.8 METHODS OF AUTHENTICATION IN INTERNET BANKING

Financial institutions providing any type of internet banking services must have effective, accurate and trustworthy methods to identify and authenticate customers. A
reliable identification and authentication system is must for complete privacy of customers' information, to avoid unauthorised financing. The risk of dealing in banking transaction with unauthorised and unidentified personnel can result into financial loss and loss of reputation of the banks.

There are numerous methods and technologies which financial institutions can use to check the authenticity of customers. These methods cover the use of customers' passwords, PINS i.e. Personal Identification Numbers, use of digital certificates with the help of public key infrastructure, physical tools such as smart cards OTPS i.e. one time passwords, biometric identification and many others. The choice of authentication method varies from institution to institution. It depends upon the outcomes of organization's risk assessment process. Currently authentication technologies include basically 3 factors.

They are as follows:

1. Something that customer knows i.e. password or PIN. If customer enters correct PIN or password, access is granted;
2. Something that customer has (may be ATM card or smart card);
3. Something about the user (biometric proof such as fingerprint, voice pattern or eye veins of user. Such biometric makes installation of specific hardware mandatory.)

There are two types of authentication methods i.e. single factor authentication method and multifactor authentication method. It is difficult to compromise on multifactor authentication method than single factor method. Multi factor authentication methods are comparatively more reliable and are greater fraud detectors provided they are perfectly designed and efficiently implemented. For e.g. in case of single factor authentication customer uses only login ID password. But in case of multifactor authentication like in ATM customer uses something that he has i.e. card along with something that he knows i.e. PIN.

But the failure or success of any authentication method depend not only on its usage but also on banking policies, procedures and controlling measures. An efficient authentication process should also win users’ trust and acceptance.
**RISK EVALUATION:** The selection of suitable authentication method should begin with an evaluation of risk posed by the banks’ net banking system. Such risk should be assessed in the light of status of user whether retailer or commercial user, banking capabilities i.e. loan transactions, bill payment, the ease of using any method and the number of transactions.

Before implementing any authentication method and tools it should be ensured that it is appropriate for the banks’ all net banking based products and services. Marketing of different products and services through internet banking involves different level of risk. Therefore, the level of authentication utilised by the banks should be according to the level of risk involved in selling that particular product or service.

A result oriented approach to authentication system requires compliance with banks information security standard, Coordination of authentication method with banks’ security environment. Any financial institutions authentication process must be consistent and it should support overall security infrastructure of the bank. With the passage of time and development of technological procedures, the authentication process should be reasonable enough to match technological changes. Although single factor authentication tools are widely used in executing variety of net banking transactions like mini statement and account inquiry, payment of bills; banks should check the authenticity of such single factor techniques keeping in mind the type of frauds emerging in virtual banking for example phishing and Trojan horse. Whenever risk evaluation indicates that single factor authentication tools are not adequate they should execute multifactor authentication process to avoid these risks. The risk evaluation process should be:

1. Able to identify all the types of dealings and the degree of admittance related to net banking products and services;
2. Able to not only recognize but also evaluate the threat managing techniques which involves confirmation tools and techniques installed for each type of transaction and access level;
3. Able to judge the efficacy of risk management modes and methods for present and varying aspects for different types of transactions and access levels.

**MONITORING AND REPORTING:** An occurrence of unauthorised access to computer system or user accounts can be determined through monitoring system. A reliable authentication method should have all the auditing features which can aid in the detection of fraud like unauthorised password or money laundering. The usage of audit logs on regular basis assists banks to reveal unauthorised activities, detect intrusion. Besides this banks should also report any suspicious transaction to proper regulatory and law enforcement agencies in order to meet the requirement of bank secrecy act. Bank should rely on various layers of controlling measures to protect the users’ information. For instance, a bank may analyse the transactional behavior of consumers for identifying any doubtful activity. Once something suspicious has been monitored and identified then efficient reporting mechanisms are required to immediately report security officials.

If at all monitoring systems and processes are outsourced in the market then it should be ensured that suitable logging and supervising procedures are employed and suspicious and fraudulent acts are communicated to the institution on accurate time. A separate auditor, may it be internal or external should access the activity report which exhibits the security coordinators’ dealings providing the required supervision for maintaining the safety of the system.

**AWARENESS OF THE USERS:** Although already initiated financial institution should make efforts to alert their customers on a regular basis. Since users’ awareness is the most powerful defense to avoid any fraudulent act, banks must review their consumer education processes and methods to know if any additional efforts are to be taken. Officers and administrators at higher and management level should organize customer awareness programs from time to time and should assess its impact. There are numerous methods to assess the impacts of these educational programs like recording the number of customers who report fraudulent acts of obtaining their confidential
details, in the websites the number of clicks on information security link, the number of mails directly received.

**TECHNIQUES OF CUSTOMERS AUTHENTICATION:** The choice and installation of any authentication technique is made depending upon the evaluated threat coupled with internet banking merchandise.

1. **SHARED SECRETS:** This is the information which is known to both the users and the banking officials responsible for authentication. For example, Passwords and PINS. Besides this there are some more examples of shared secrets techniques which are discussed as follows:
   a) There are certain questions that require specific user knowledge to respond or to answer like the accurate amount of the customers EMI.
   b) A particular picture or an image selected by the customer must be identified from a given list of imagers. The choice of users shared secret is generally done at the initial stage while logging. Shared secrets can be changed over a period of time with proper information to the authentic entity. These shared secrets which are never changed are termed as “static”. In case of static shared secrets the chances of risk increases. But if the customer uses multiple shared secrets, it enhances security because then user must know more than one single secret to log in or authenticate.

2. **TOKENS:** Something that the customer has may be physical devices are referred as tokens. There are three types of tokens which are explained in great detail as follows:
   a) **USB Token Device:** size of this tool seems to be exactly like a home key. This tool can be straight plugged inside USB part of the computer. Thus, it does not need fitting of a particular hardware on the customers’ supercomputer. If this tool is identified then user is supposed to type one’s passwords to gain access with the computer system. It is difficult to make duplicate copy of USB tokens being single piece; comparatively they are secured devices for storing and safeguarding confidential information. USB token is a user friendly device because it is easy to
carry and since it directly plugs into computers USB port, it does not require any additional hardware.

b) **Smart Card**: size of this automated card and size of a credit card seems to be similar. It has a microchip which stores and processes data. Availability of microprocessor helps software developers to install efficient authentication schemes. In order to use smart card, it has to be inserted into compatible reader which is connected to the computer of the user. Once the authentication entity identifies smart card to be valid, user is supposed to type in ones password to complete the process of authentication.

Although smart cards are easy to carry and safeguard the confidential information the key disadvantage of this device that it requires a special connection of hardware and related software devices on computer system of the customer.

c) **Password Creating Token**: a unique password is generated which is also known as one time password (OTP). It is ensured through this method that the same OTP is not used consistently. There is a small screen on the token which displays OTP. The user primarily enters ones user name and regular password and then the OTP which is generated via this tool. The authentication of the user becomes successful if match is found between usual password and token generated OTP. In certain systems OTP is created at the interval of 60 seconds or sometimes 30 seconds. The time period for which password is created is known as the life span of password. The OTPS are generated randomly. Similarly, their unpredictability and uniqueness makes it difficult for the fraudsters to capture and use OTPS generated from keyboard logging.

3. **BIOMETRICS**: under this method identification and authentication of a customer is done on the basis of physical attributes like what a customer is. Physical attributes include facial structure, iris configuration, fingerprints and pattern of movements like the way in which user enters data on a keyboard of the computer. First the users are enrolled or registered for biometric based technology. In the process of registration/ enrolment samples of physical attributes of user are converted into mathematical model which are also referred as templates. After these templates are stored in to database, software
performs analysis. Once the customer is registered, on log in he or she is connected to biometric technology and thus physical attributes like fingerprints are compared with those templates which were registered in advance. If they match, authentication is complete and customer is granted access.

Biometric identification is a part of multifactor authentication system. This is because it is a combination of physical attributes (i.e. something a user is) with password or a token (i.e. something a user knows or has). There are numerous biometric techniques which are used for authentication. They are listed as follows: Retinal scan; Voice recognition; Fingerprint recognition; Iris scan; Keystroke dynamics; Facial recognition; Finger / hand geometry.

- **Retinal scan**: this technique quantifies the blood vessel configuration in the posterior area of the eye. Usage of this technology requires still (without any movement) standing of the user just near the device which shines a light source into his eyes. The weakness of this biometric is that retina may change under peculiar medical condition like high level of blood pressure, pregnancy.

- **Voice recognition**: This technique involves use of vocal features to identify an individual. This technique is not completely developed within itself because noise in the background may affect the performance. The most commonly accepted biometric techniques are face and fingerprint recognition.

- **Recognition of Fingerprint**: Amongst all the techniques of authentication, fingerprint is the ancient and ink used method, successfully used in various applications. Everyone possesses distinctive fingerprints. In this technology analysis is done of minutiae. It means analysis is done not only of small unique marks along with ridge endings but also of the branches which exist in the ridges of the fingerprint. Information which is gathered through fingerprints is very minute and solid. Therefore, fingerprints are most trusted method of authenticating the customers’ identity. In this technology data related to small unique marks i.e. fingerprint minutiae is only stored and entire pictures of actual fingerprints are discarded. Scanners required for fingerprint may
either be built into keyboard of computer or pointing devices like mice or may be separately connected to a computer. Fingerprints are most accurate and complex enough to be a reliable template for authentication. If multiple fingerprints are obtained from an individual it facilitates higher degree of accuracy. Amongst various biometric methods fingerprints are the most accurate and reliable techniques. Usage of fingerprint technology requires installation of not only appropriate hardware but also software on the user’s computer system. Since scanning device is attached on the customers’ computer itself this technique is not portable. Compared to iris scanning fingerprint technology is easy from both installation as well as usage point of view. Registration or enrolment of the users can be done at the organization’s customer service centre or after the user has received instructions and password. According to the vendors of this technology although once enrolled, it provides enough security, for transactions involving a higher amount of dollars financial institutions should make the user remain present physically.

- **Iris scan**: this technique is highly accurate as well as user friendly. Iris is an internal organ whose texture is unwavering throughout one’s life. Therefore, it can play the role of living passport or a PIN. Being an internal organ, iris is invulnerable to environmental effects excluding its papillary reaction to the light. No iris patterns are identical. Even iris pattern of one’s left eye is not the same as that of the right eye. This method of recognition is highly trustworthy method for verification. Although expensive, it can be fruitfully used not only for identification but also for authentication in internet banking.

- **Keystroke dynamics**: keystroke authentication is a computerized system of assessing one’s keystrokes on the keyboard. This method observes speed and pressure of keystrokes, time taken for typing a password. The procedure of this technology is still in the developmental stage to improve its uniqueness.

- **Recognition of Face**: face recognition is a robotic system to note the peculiar characteristics of someone’s face. Although several vendors have various methods of
face recognition, almost all of them emphasis on specific facial features. Newly invented methods constitute maps of three dimensions. The technique clicks images of faces with video cameras. Then templates are generated and stored and later utilized for comparisons. Scanned images of faces depend on the environment in which they are collected. The best images are captured in controlled environment with suitable lightning and proper angle of video camera. To be on higher security zone numerous cameras can be installed which may capture images from various angle. There are many facial scanning applications which cover test of liveliness like blinking eyes. Liveliness testing reduces the risk of unauthorized access.

- **Finger / hand geometry**: it as a mechanical measurement of numerous angles of the hands and finger. None of this dimension includes palm or fingerprint. Infact, simply spatial geometry is observed when one lays his hand on the surface of the sensor. This method practices two or three fingers. This technique is exhaustively trialed and accepted by the users without objections. Hand and finger geometry observation depends upon the dimension of the hand structure. If compares with other techniques of biometric, the correctness of this technique is at little lower level but yields a very little FRR i.e. false Rejection Rate. Simple and basic cost operational setup is main positive point of hand / finger geometry biometric. Hand biometric is most popularly used for attendance or time notations in institution and organization.

Thus, the biometric avails further more security over the present multifactor authentication system which is used in internet banking to execute transactions from a computer.

4. **OTP password scratch card without hardware**: Scratch card is one of the methods of existing authentication technologies i.e. something a user has. Scratch card are not much expensive. This card looks like a bingo card and it contains letters as well as numbers which are arranged in row and column format. This format is exactly like a grid. The cells in the grid depend upon the size of the card.
As a technique of authentication process, the user is primarily supposed to enter one’s own identity in the form of not only one’s name but also secret password in proper way. Once this requirement is entered accurately, then user would be instructed to enter the characters in the cells of the grid as a second authentication factor.

Traditional one time password tokens depend on electricity which may fail due to some fault. Yet if the grid is installed on a wallet size plastic card, it becomes durable as well as portable. This technique of authentication does not require any training and if at all the card is misplaced, it can be replaced with ease and at a lesser cost.

MUTUAL AUTHENTICATION: In this process not only users’ identity is authenticated but also the website of the financial institution is authenticated to the users. At present almost all the banks don’t authenticate their websites to the users prior to confidential information collection. One of the major reasons behind success of phishing attacks is that users are unable to recognize that they are being misguided to fraudulent websites during attack.

The fraudulent websites are so well constructed and executed that it becomes difficult for the customers to doubt on their authenticity. Here, banks can help their customers in understanding difference between original websites and spoofed websites by authenticating the former one.

TECHNIQUES FOR USER VERIFICATION:
User verification is although associated, different from that of process of authentication. User verification is followed by authentication process and it should be done at the time of originating the account. Personal information can be verified in the following three ways:

- Positive verification: It implies an assurance of matches between details provided by the customer and the details available from the sources of trustworthy third party. To be more specific it means that banks can check the identity of a user by making a
comparison between the answers provided by the user and the information stored in the trusted database. If the questions are specific perfect answers boost the confidence level of the banks that the user is one whom they are thinking of.

- **Logical verification**: to assure that the details entered are sequentially steady, for example whether address of the street, depending upon the area telephone code and PIN code are same.

- **Negative verification**: - this verification includes the act of ensuring that details provided have not been related to any fraudulent activity in the past. For e.g. Information entered by the applicant can be compared with any fraud database to find out if any fraud of such behavior existed in the past.

One of the authentication methods is that of banks’ dependence on outside vendor for verification of customer’s individuality (uniqueness). In this method an electronic credential like digital certificate would be issued by the third party to the customer to prove ones identity. In such a case it becomes banks responsibility to assure that degree of authentication used by the third party should be same as that of the bank itself.

### 1.9 PROBLEM ON HAND

Scholar reviewed a huge amount of literature and visited almost twenty private banks in the western regions of Mumbai. While going through the literature research scholar concluded that there are various types of risks associated with internet banking. At the same time as a precautionary method RBI has given numerous guidelines also to avoid these risks. Authentication technique is one amongst those guidelines. Several authentication techniques have also been referred by the research scholar while reviewing the literature as mentioned above. Even after so many encouraging factors scholar observed past general discussion with people of western regions of Mumbai that internet banking although used by masses not at a larger scale. There are people
who are happy and contented with debit card, credit card and Automated Teller Machine facilities. They are not bothered to use internet banking at maximum possible times. Different users have different view on acceptance of internet banking. Although people are using internet banking, security concern is affecting their level of usage. Researcher also realized that banks also play an important role in making the users accept internet banking in true sense of the word and then using it on a larger scale.

Even though virtual banking is observed as an usual habit in developed countries namely United states of America, United Kingdom and other European countries, in Indian economy it is yet at the blossoming stage according to Bashir & Madhavaiah (2014).

Keeping all the above observations in mind scholar selected the current topic for her research i.e. “Study of Electronic Banking with Special Reference to Internet Banking in Private Sector Banks.”

1.10 SCOPE OF THE RESEARCH

The present research dealt with level of usage of internet banking and consequently levels of satisfaction derived from the same. The study also analyzed the internet banking users’ views with respect to their age, gender and cost structure. Almost 15 private banks have also been interviewed by the researcher along with 300 respondents from western regions of Mumbai from Andheri to Borivli.

RESEARCH GAP:

End numbers of theoretical background have been reviewed by the scholar. Various analyses as well as conclusions have been observed as factors determining usage of armchair banking services. Common attributes noticed were emphasis either on user or
nonusers of net banking services. Not much analysis has been done on the levels of access. May it be operational or frequency access. Rarely satisfaction has been analysed with clarity on operational and security dimensions. Therefore, this extensive research aims to analyse in detail attributes of satisfaction and levels of access.