ISSN No. 0976-5697

Volume 6, No. 5, May - June 2015

International Journal of Advanced Research in Computer Science

REVIEW AERICLE

Available Online at www.ijarcs.info

# Internet Banking Technology in Banking Industry

[1]Prof. Minakshi Bhosale. [2]Dattatraya Bhosale
[1,2]Shivaji University Kolhapur
Head, Dept. of MCA, YSPM's Yashoda Technical Campus, Satara
Maharashtra, India.

***Abstract:*** - Internet banking can improve a bank's efficiency and competitiveness, so that existing and potential clients can take advantage of a greater degree of convenience of successful transactions. This increased level of convenience, when combined with new technology, can enlarge the bank's target customers. As a result, banking industries are more aggressive in implementing Internet banking capabilities that include sophisticated advancement systems. Internet banking has added another measurement to bank transactions by permitting clients to lead monetary transaction through the Internet. The remarkable rate with which new innovations are, no doubt embraced, the omnipresent and worldwide nature of electronic systems.

Banking institutions have taken numerous suitable measures to safeguard security of Internet banking. Nevertheless, it is also essential along with the part of clients to follow some simple, yet important methods to prevent themselves from becoming a victim of computer crackers, who can gain illegal access to the Internet bank accounts. The purpose of the above research paper is to provide detail information about Internet banking technology to the customer. Through this information customer is aware about this service and take a benefit of this service.

***Keyword:*** - Internet banking, Delivery channels, Information security, Technological risk, Risk management

## I. INTRODUCTION

The origins of the Internet are rooted in concerted government sponsored efforts to promote science and technology; especially by the US military industrial complex. In year 1969 the Pentagon's Advanced Research Project Agency (ARPA) launched a project to merge computer and telecommunication technologies in a global data-sharing and information-exchange network for scientists. Advanced Research Project Agency Network (ARPANET) was expanded in 1989 and creates a wider network infrastructure known as a World Wide Web in 1990. Globe is shifting rapidly and taking on such changes only technological development is to be considered. For the progress of our life technology is the key aspect to be utilized. Now a day, every task can be carried out at home or at the workplace, handled by electronically because everyone is accepting information technology as a key for success [1]. The Internet is a global phenomenon used by everyone to execute the work fast at any time and even at any place. The transformation from the traditional banking towards e-banking has been a 'leap' change [2].

Internet banks rely more heavily on non-interest income and less on core deposits for funding than non-Internet banks. For the smallest size banks, Internet banks have better accounting efficiency ratios and higher returns on equity than non-Internet banks. Internet banks with assets under $100 million had a significantly worse accounting efficiency and profitability ratios compared with non-Internet banks of the same size.

Internet banking is helpful for the customers, financial institutions, individuals or business to access account information to perform business transactions by using a public or private network. It can give a number of advantages, but on the other side the risks are more. Banks require keeping a balance between benefits versus risk. Now a day in the market bank gets customer immediately, but customer continuously attached to the specified bank is a challenge to the bank and for that they need a great deal of homework to be managed.

## II. EVOLUTION OF TECHNOLOGY IN INDIAN BANKING SECTOR

Internet banking is the robotic delivery of banking products as well as services provided directly to the customers through electronic media and interactive communication channels. Because of optimization, customers have profited from a bigger degree of convenience in banking transaction. Internet banking can improve efficiency in the work and competitiveness. Nowadays, due to fast, accurate new services the customers of the banks are increasing. Hence banking industry is becoming more aggressive in launching Internet banking services in the bank.

Table 1.2 Growth in the technology

| Sr. No. | Year | Growth in the technology |
|---|---|---|
| 1 | 1960 | Mechanized Banking |
| 2 | 1970 | Computer based banking |
| 3 | 1980 | Computer-linked communication based banking |
| 4 | 1983 | Use of Advanced Ledger Posting Machines (ALPM) in every branch of banks |
| 5 | 1994 | The use of EFT is started. Increase the use of Magnetic Ink Character Recognition (MICR) at branch level. |

(Source: -[3])

One day technology development is increased and customer requires fast quality oriented service at minimal cost. Hence bank moves towards the evaluation of Internet banking technology at branch level. Nowadays to balance the technology with cost investment and risk associated with this technology are the biggest challenge to the bank. From the customer side proper understanding of the Internet banking technology is important and, from the bank side, bank should prepare a project plan and supervise execution of this plan to achieve business profitability is mandatory to increase the scope of this technology. Recently, e-banking has become increasingly important in banking activities. The main reasons include modern technologies, the expansion of competition, and the need for efficient and comfortable services, cost and economic changes [4].

Following are the essential market factors through that bank turn to the Internet banking technology.

a. Worldwide competition is increasing in the market due to the globalization. Cost reduction and revenue enhancement are the foremost motives for banks to turn towards Internet banking. Banks use Internet banking to possess existing customers loyal successively towards the bank and approach new customers regularly to the bank.
b. Cost efficiencies are the basic reason for Internet banking progress. Bank branches as well as the customer can deliver banking services on the Internet at very low transaction prices as compared to traditional banking at a branch point. The actual price to implement a banking transaction depends on the distribution channel used by the customer for performing the transaction.
c. Geographic Scope allows the client to use Internet banking services and products with minimum cost and high speed. There is no any problem from which place customer can do the transaction. In fact, some banks are virtual banks. They are doing their business entirely via the Internet. They do not have any traditional banking office. They communicate their customers online.
d. Brand name is the grace of today's universal business. The primary purpose of every marketable enterprise is to give uppermost priority to keep up an association with the client. In the same way the banking institutions are also taking a one step ahead. The bank can develop enduring connections with customers and build customers trustworthiness to enhance business activity through Internet banking.
e. A customer demographic play important role in the banking industry. Customer of Internet bank uses a variety of services provided by the bank. Few of bank customers are believed only on traditional banking transactions. They believed that it is a more prosperous way to execute banking transactions and a form of opinion that customer to customer touch is an important fundamental aspect in every winning business. Other clients are believed in innovative technologies. They are using their own PC with an Internet connection through that they enjoy the banking services regularly. To understand the proper customer demand and according to that demand provides a proper delivery channel is a great challenge for all depository financial institutions.

## III. TYPES OF INTERNET BANKING

On any platform, Internet banking application executed with different architecture. Branch level atomization banking product utilizes centralized or distributed architecture. It also uses a client server or three tier architecture based on a file system or a DBMS package which allowed the customer different levels of access to a variety of facilities.

***a.*** ***Information only systems***- with this type of Internet banking overall information about customer, interest rates, branch localities, product geographies loan, and deposit interest calculators are provided in the bank's website. These websites allow the customer to download different application forms of bank services. In this type of information system customer can send emails to solve any problem or get information about any queries. These sites cannot identify an authenticate customers. No any type of transaction and interaction performed on bank data.

***b.*** ***Electronic Information Transfer System***- In this type of system bank provides the customer facility of reading only information; such as personal information, account balances, transaction details, statement of accounts, etc. In this method password, a proxy server is a simple technique used for the authentication. Data accesses in bank site are entirely in offline mode.

***c.*** ***Fully Transactional System***- In this type bank allows customers to perform online transaction through that the customer can update his bank account information. Due to financial data, this type of system requires strong security and control systems for secure financial transaction. The performance of this system requires appropriate technology, networking, inter-bank payment gateway and legal infrastructure.

## IV. INTERNET BANKING DELIVERY CHANNELS

Different delivery channels used by the Internet banking are as follows:

### *A. ATM:*

Automated Teller Machine (ATM) was a computerized telecommunication device used by a customer to withdraw amounts from his account at any time and in a public place. In an ATM center customer is identified through the plastic ATM card with a magnetic stripe or a plastic smart card with a chip, which contains a unique card number and some security information, such as an expiration date or Customer Verification Code (CVC). For the security purpose customer uses a Personal Identification Number (PIN) [5].

### *B. IVR (Interactive Voice Response):*

Interactive Voice Response is the automatic voice response system used by the customer to check their account balance or recent transactions by simply dialing a toll-free number any timewhen the need arises [6].

### *C. CDM (Cash Deposit Machine):*

Cash deposit machines can offer significant benefits to both banks and their depositors. According to "(April 2012) Indian banking industry" report the machines can enable depositors to deposit cash at more convenient times and places them during banking hours at branches. At the same time, by automating services that were previously filled out manually, CDMs can reduce the costs of servicing from depositor demands. These possible benefits are multiplied when banks share their CDMs, allowing depositors of other banks to access their bills through a bank's CDM.

### *D. POS (Point of Sale):*

Point of Sale is used for retail transaction. The client performs a transaction by swapping the card on the POS machine. Most of the customer use debit or credit card for purchasing products. Different payment gateways offer their services to banks such as VISA card, Master Card etc. [6].

### *E. Online Payment Systems:*

The online payment scheme means to transfer money between a buyer and a vendor in a transaction. For the secure transaction, the bank needs to follow proper rules and procedures. The payment system provides an infrastructure for transferring money from one entity in the economy to another.

Electronic payment systems are of two types such as wholesale payment systems and retail payment systems. In wholesale payment system transaction performed between banks, corporations, governments and other financial service firms. It is also called as Large Value Payment Systems that handle a large volume of payments with relatively minimal cost. Retail electronic payment system transactions performed between two consumers.

There are two types of wholesale payment systems these are Net settlement systems in which the settlement of funds transfer occurs on the Internet, according to the rules and procedures of the system. The net position at the settlement time can be a net credit or debit position. The second type is the Gross settlement system in which the settlement of funds occurs on a transaction basis, that is, without netting debits against credits [7]. Following are the widely used online payment systems

#### *a. First Virtual:*

First Virtual’s system does not rely on any form of cryptography, or necessitate any extra hardware or software. Clients must accept an Internet e-mail, and a valid VISA or MasterCard, which is conducted initially by phone to the first virtual. The first virtual assigns a virtual PIN to a customer, who in turn uses this virtual PIN instead of a credit card number to place an order with a merchant. First Virtual’s type of operation, where a third party processes credit card transactions, is called a ‘factoring’ operation, which according to VISA International guidelines is against the law [8].

#### *b. DigiCash:*

David Chaum, a mathematician and privacy expert, founded DigiCash. He created e-cash, proprietary electronic cash tokens, which are marketed as being the equivalent of cash. An account is established at a DigiCash-licensed bank with real money. Once established, the customer can withdraw e-cash that is stored on the user computer's hard drive. Using proprietary software, e-cash can be spent with an Internet merchant or with anyone else, whose computer is set up to deal in e-cash. Using public-key cryptography, the digital tokens are considered to be insecure and can be registered and verified by the issuer without revealing to whom it was originally issued. In effect, these digital cash transactions are in a position to anonymous as cash. No transaction confirmations are necessary; it means that the merchant can immediately ship the product [9].

#### *c. Cyber Cash:*

This payment mechanism consists of a downloadable software package using public-key encryption that is designed to assure the security of credit card transactions over the Internet. The system protects the customer's authentication data. An account is set up and acts as an Internet front end to an existing credit card that is designated. When a purchase is made, copyrighted software is used that sends the purchase and account information in encrypted form to the account provider. The provider in turn sends the information to the appropriate financial organization for processing [9].

#### *d. Net Cash:*

This concept is similar to e-cash, except that it does not prescribe any special software to be utilized. Net Cash is transmitted across the Internet using an encryption scheme known as PGP (Pretty Good Privacy). To get net cash, a party must send a cheque or money order to the company's headquarters. The company returns electronic coupons via email [9].

#### *e.* ***Net Cheque:***

Net Cheque offers a user friendly and secures way of writing an electronic cheque by offering PC software to its registered customers. Before transferring an electronic cheque over the Internet, Net Cheque system security replaces the confidential bank account information with a shadow account which is used to determine the account information to the transaction processing segment of the system. The electronic cheque is then transmitted across the Internet to a closed system for processing. Once the electronic cheque is received on the private system, the cheque is verified for authenticity and the shadow account is replaced with the actual consumer and merchant information. After the transaction is completed, an email is sent to the customer for confirmation [9].

#### *f.* ***Millicent:***

The Millicent method was developed by Digital Equipment Corporation (DEC) to manage small payments (e.g. Payment for getting information from the Internet about news and stock quotations or payment for small programs like Java-applets).

The customer buys broker script with a defined value by using his credit card or by debiting a suitable bank or brokerage account. Such script is like a telephone card. At the time of purchase, the customer exchanged parts of the script into a dealer's script. This script is then sent to the dealer. The dealer collects all scripts and exchanges them into "real" money.

#### *g. Electronic Checking Accounts:*

Numerous organizations have been trying to create ways of utilizing existing checking accounts over the Internet. In most of those efforts, the consumer uses his or her checking account with a bank or service and then draws down those funds using special electronic cheque and digital signatures. Generally, these programs were not that close to a major commercial introduction as are those based on credit cards. Many observers feel that electronic cheque, despite a slow start, could become a widely used method for making payments.

### *h. Credit Cards:*

The credit card is usually a four-party card which involves two banks in each transaction, the cardholder's bank (the issuer of the card) and the retailer's bank. The retailer hands over the credit card slips to its private bank for payment, less a discount, typically about 2-3%. The retailer's bank then passes the slips onto a clearing system. The clearing system presents each slip for payment to the bank that issued the card on which it was written. The issuing bank collects from the cardholder. All of these exchanges are now done through the Internet.

### *h. Debit Cards:*

With a debit card, the payment comes right out of your checking account. The card is available to the entity that holds your money on deposit, probably a bank. When you introduce your card, money is moved from your account to the merchants account on the same day.

### *i. Stored Value Card Schemeor Smart Cards:*

Smart card technology represents a real change in how and where information is processed. The smart card brings huge credit card-sized payment mechanism with an integrated circuit chip embedded within the card. The embedded chip enables the card to contain a significant amount of data including prepaid stored value. The embedded chip can also hold programs that interact with data either contained on the chip or external to the chip. These programs can be permanent and unchangeable or can be modified when the card is plugged into a network. Data can be stored, updated and retrieved both when the card is issued and throughout its life.

However, due to the embedded chip, the smart card operates as a standalone payment mechanism in effect, a direct substitute for cash without requiring online network connections. This stored value can be accessed and altered by terminals at a merchant's establishment or at remote locations. A consumer with a smart card can go to a bank or ATM and have the card loaded with a certain amount of value. The consumer can then proceed to make purchases up to the amount of stored value, in the same manner as if the currency were being used. At each terminal, the device reads the smart card to signify that there is sufficient value available and deducts the amount of the transaction. When the card's value has been exhausted, the customer can return to the bank or ATM to replenish the value.

The strength of this scheme is the fact that it avoids the need to identify the user and access the user's bank account or credit card in order to verify funds availability because the only funds available are those that are on the card. This eliminates the problem of retailers who are unwilling to accept payment by cheque due to concerns about funds available.

### *j. Mondex:*

The Mondex electronic cash system operates on a smart card and the microchip contains a purse in which the Mondex value is held electronically. The purse consists of five separate pockets, allowing up to five different currencies to be held on the card at any one time. The microchip also contains the Mondex security programs which protect transactions between one Mondex card and another.

Since information is in digital form, Mondex transactions can be carried out over a telephone line or the Internet. The microchip maintains a record of the last ten transactions and the electronic cash can be locked in to the Mondex card using a code chosen by the user. Mondex electronic cash can be transferred directly to a retailer, merchant or other outlets to pay for goods or services, and like cash, Mondex enables transactions between individuals, without the need for banks or other third parties.

## V. APPLICATIONS OF INTERNET BANKING

Internet banking solutions have following applications:

a. The customer can monitor his account transactions for sitting at any place.
b. Customer of bank can transfer money from his account to any person's account.
c. Inter-bank fund transfer is possible.
d. Safeguarding of future fund transfers and beneficiaries.
e. The customer can update profile, change account correspondence address whenever want.
f. For security purpose customer changed password regularly.
g. For any problem or specific inquiries, send message to Internet banking customer care.
h. The customer uses different facilities such as stop check facility, cheque book request, cheque return inquiries, cheque deposit inquiry, current account statement request, profit rates inquiry
i. Customers make payment of bills to service providers.
j. Customers open a Fixed Deposit online through fund transfer.
k. Recharge your prepaid phones.
l. Perform shopping online for all kinds of products, make railway passes for local trains online.

## VI. BASICPRINCIPLES OF INFORMATION SECURITY

In information security mechanism consists of confidentiality, integrity and availability these are the core principles and other side authenticity, non-repudiation and accountability are also now becoming key considerations of information security.

***a.*** **Privacy** is nothing but to secure unauthorized access of a transaction from an unauthorized person. Now in banking transaction and shopping we need to maintain the secure credit card number when it transfers from the buyer to the merchant and from merchant to transaction processing network. In this case, credit card number is encrypted and transfer to the transaction processing network.

***b.*** **Reliability** is nothing, but data cannot be modified without authorization. Only authorized user can make the changes to the existing data. Suppose any user can deduct amounts from the other user account without authorization, then this transaction cannot perform due to integrity function.

***c.*** **Convenience** is nothing, but the information required for a customer for any purpose is available any time when needed. Computer system is used to store and process data securely when it is transferred through a communication network. Avoid unauthorized access and data is available whenever required.

*d.* **Authenticity** occurs when information transfers from the buyer to the merchant and the merchant to the buyer. The sending and receiving of information can be performed authentically. Unauthorized users cannot break the secrecy of information when it is sent.

*e.* **Non-repudiation** is nothing, but to fulfil one's obligations under a contract or transaction. Electronic commerce uses technology such as digital signatures and encryption to establish authenticity and non-repudiation.

*f.* **Identification** is the way to tell the system who you are. User can enter the account name and number to identify the authorized user. If the customer entered account name and password matches with the stored customer account name and number, then only open the account and do the transaction otherwise no one can execute the transaction

*g.* **Authorization** is nothing, but the privileges or authorizations assigned to the user for retrieving the transaction. If the user has altered the permissions, then modifications can be performed by the user and above customer is authorized user. Otherwise access is denied not any modification is possible.

*h.* **Accountability and auditability** are the key considerations of Information security. Organization security policy can be properly enforced only if accountability is maintained, i.e., Security can be maintained only if subjects are held accountable for their actions. Effective accountability relies upon the capability to prove a subject's identity and track their activities. Accountability is established by linking a human to the activities of an online identity through the security services and mechanisms of auditing, authorization, authentication and identification. Thus, human accountability is ultimately dependent on the strength of the authentication process. Without a reasonably strong authentication process, there is doubt that the correct human associated with a specific user account was the actual entity controlling that user account when an undesired action took place[10][11][12].

## VII. THREATS OF INTERNET BANKING

Internet banking in India is in its initial stage of development. Most of them are offering basic services only. The deregulation of the banking industry coupled with the emergence of modern banking technologies is enabling new competitors to enter the financial services market quickly and efficiently. Internet banking challenges are summarized below.

a. Nowadays to increase the customers of the bank, proper understanding of the customer requirements is the biggest challenge of every bank

b. Technology development and customer awareness was grown significantly so banks need to offer transparent services to their customers

c. To maintain a breach of privacy to identify the authorized customer is a big challenge of the bank

d. Now a day's use of the Internet grows exponentially. For sensitive transaction, speed and high bandwidth are the necessary part. So Internet banking success only has the proper infrastructure comprising telecommunications and bandwidth

e. Awareness of computer technology for Indian people is very poor and computer literacy in India is still very low: Computer awareness of Indian people is very poor and is one of the barriers to faster acceptance of Internet banking

f. The mind-set of the Indian customer needs to be changed towards Internet banking.

g. The unauthorized access of a customer account to change information through cracking login and passwords is a common way of fraud

h. Denial of services: millions of queries can block computer network. Some cases of electronic damage involve the actual destruction or disabling of equipment or data. Turning off power or sending messages to system software telling it to stop processing. Such type of attack is called denial of service attack

i. When data are transmitted from the sender to the receiver, the data can be changed in an unauthorized manner. For example, customer doing fund transfer, then the transfer amount will be changed. Customer can receive bills of higher amounts than the actual transactions this is known as data diddling

j. Session hijacking is the big challenge of the Internet banking technology. Hijackers are the unauthorized mediator between the server and the client. They can hijack the data and make it impossible to reaching the destination. During online transaction hackers hack the credit or debit card number. They can thus enjoy the full benefits of the card without being an actual cardholder

k. The preliminary cost of Internet banking is high. It includes the cost of connection to the Internet or any other mode of electronic communication, cost of the required hardware, software and other related components like modem, router, bridges, network management system, cost of maintenance of all equipment's, web sites, skill level of employees, the cost of setting up organizational activities etc.

l. To provide 21 hours quality oriented services to bank customer bank required well qualified, highly skilled employee base to meet internal or external needs. Hence bank requires investing in training of new technology and proper maintenance of equipment required for the efficient service of Internet banking to customer

m. To perform proper Internet banking transactions bank need skilled personnel working in banks. But now a day's lack of skilled personnel such as a web developers, content providers and knowledgeable professionals to route banking transactions through the Internet

n. The low percentage of customers using Internet banking, as well as the relatively modest cost of setting up an Internet banking Web site, make it unlikely that Internet banking is having a sizeable positive or negative impact on the bottom line of most institutions. However, an exception to this generalization might be found among the handful of large banks with a disproportionately larger share of Internet banking [13].

These are unique challenges faced by the banking industry to adopt successful Internet banking technology in their banking sector.

## VIII. TECHNOLOGICAL RISK OF INTERNET BANKING

Every coin has two sides. Every good thing has bad side, or benefits have disadvantageous side. Technology is a basic need of modern life, but it should be not neglected that there are some risks in using technology; especially there is the most considered risk in Internet banking such as:

***a.*** ***Hacking*** - It is the activity of breach on a computer system to gain unauthorized access is the hacking. The act of defeating the security capabilities of a computer system in order to obtain illegal access to the information saved in the computer system is hacking through that bank customer data can be accessed unauthorized way. Another highly dangerous computer crime is the hacking of IP addresses in order to transact with a false identity.

***b.*** ***Phishing -*** It is the act of gaining sensitive information like username, passwords and credit card details of customer those are doing an online transaction. Phishing is performed through emails. It will force the user to enter personal information through fake websites

***c.*** ***Computer viruses*** - These are the unsafe computer programs which replicate themselves and harm the computer systems on a network without the knowledge of the system users. Through the network file system, network, Internet or any removable devices like CD’s, DVD’s, and USB drive viruses spread from one computer to another.

***d.*** ***Cyber stalking*** - cyber stalkers use the Internet as a communication technology to torture other individuals and it is known as cyber stalking, false accusations, the transmission of threats, damage of data and equipment fall under the class of cyber stalking activities. Cyber stalkers often target the users by means of chat rooms, online forums and social networking websites gather user information and harass the users on the basis of the information gathered.

***e.*** ***Identity thefts*** - These are one of the most serious frauds as it involves stealing money and obtaining other benefits through the use of a false identity. It is the act of pretending to be someone else by using someone else’s identity as one’s own. Financial identity theft involves the use of a false identity to obtain goods, services and commercial identity theft is using someone’s business name or credit card details for a commercial purpose.

***f.*** ***Physical securities*** - These are concerned with the physical protection of the computer, computer equipment, computer media, and the overall physical facility from natural disasters, accidents of various kinds, and intentional attacks. Following are the breaches of security attack.

a) Dumpster diving or trashing - It is a name given to a very simple type of security attack. In this attack all kinds of confidential information turns up in the trash, and industrial spies through the years have used this method to get information about their competitors. Around the offices and in the trash, crackers can find used disks and tapes, discarded printouts, and handwritten notes of all kinds. There is another type of computer-related “trash” that you might not consider. In the system itself is files that have been deleted, but actually was erased by the system computers and computer operators is oriented towards saving data, not destroying it, and sometimes the data are saved that shouldn’t be.

b) Wiretapping- It is a number of ways that the physical method can breach networks and communications. Criminals sometimes used wiretapping method to eavesdrop on communications. It’s unfortunately quite easy to tap innumerable types of network cabling. For example, a straightforward induction loop coiled around a terminal wire can pick up more sound and RS232 communications. More complex types of eavesdropping can be formed as well. It is important to physically secure all networks, cabling to protect it both from interception and from vandalism.

c) Denial of services - A few security breaches span most of the categories. There are for two types of attacks in this category. Some cases of electronic sabotage involve the actual destruction or disabling of equipment or data. Turning off power or sending messages to system software telling it to stop processing are examples of the former type of attack-a classic denial of service. The other type of attack is known as flooding is the type we saw with the Internet worm. As the worm spread across systems and networks, it kept creating new processes that so clogged the affected systems that other work couldn’t get done. In this type of attack, instead of shutting down services, the attacker puts more and more strain on the system’s ability to service requests, so eventually they cannot function at all. Another example of flooding is the electronic mail bomb. There are many examples of accidental denial of service.

***g.*** ***Breaches of personnel security***

***a)*** ***Masquerading*** - It occurs when one person uses the identity of another to gain access to a computer. This may be accomplished in person or remotely there are physical and electronic forms of masquerading. In person, a criminal may use an authorized user’s identity or access card to get into restricted areas where he will get access to computers and data. Electronically, any unauthorized person will use an authorized user’s logon ID, password, Personal Identification Number (PIN), or telephone access code to gain access to a computer or to a particular set of confidential data files. Unauthorized password use is the most common type of electronic masquerading, and it’s a very effective one. If an outsider steals or figures out a password, there is no easy way for the system to tell whether the person who enters the password is the legitimate, authorized users, or an outsider. Passwords are too easy to crack

***b)*** ***Digital signatures and certificates-*** It meets the need for authentication and integrity. To vastly simplify matters, a plain text message is executed through a hash function, so given a value in the message digests. This digest the hash function and the plain text encrypted with the recipient's public key is sent to the recipient. The recipient decodes the message with their private key, and runs the message through the supplied hash function to that the message digest value remains unchanged. Very often, the message is also time stamped by a third party agency, which provides non-repudiation. A digital certificate is a digital document issued by certification authorities that uniquely identify the merchant. Digital certificates are sold for emails-merchants and Web servers.

***c)*** ***Secure socket layer*** - In SSL information sent over the Internet commonly uses the set of rules called TCP/IP (Transmission Control Protocol/Internet Protocol). The information is broken down into packets, numbered sequentially and error control attached individually. Packets are transmitted from different routes. TCP/IP resembles them in order and resubmits any packets showing errors. SSL uses PKI and Digital Certificates to ensure privacy and authentication the procedure is something like this. The client sends a message to the server, which replies with a digital certificate. Using PKI, server and client negotiate to create session keys, which are symmetrical secret keys specially, made for the actual transmission. Once the session keys are agreed, communication, continuing with the session keys and digital certificates.

***d)*** Peripheral Component Interconnect (PCI), Secure Electronic Transaction (SET), firewalls and Kerberos -credit card details can be safely sent with SSL, but once stored on the server they are vulnerable to outsiders from hacking into the server and accompanying network. A PCI card often added protection, therefore, or another approach altogether is adopted: SET is developed by VISA and MasterCard. Secure Electronic Transaction (SET) uses PKI for privacy, and digitally authenticates the three parties: Merchant, customer and bank. More importantly, sensitive information is never seen by the merchant, and is not kept on the merchant's server. Firewalls protect a server, a network and individual PC from attack by viruses and hackers. Equally significant is protection from malice or carelessness within the system, and many companies use the Kerberos protocol, which uses symmetric secret key cryptography to restrict access to unauthorized employees [14].

***e)*** ***Transactions*** - Here sensitive information has to be protected through at least three transactions.Credit card details are supplied by the customer, either by the merchant or payment gateway. These are handled by the server's SSL and the merchant, server digital certificates.Credit card details passed to the bank for processing is handled by the complex security measures of the payment gateway.Order and customer details supplied to the merchant, either directly or from the payment gateway. The credit card processing company is handled by the SSL, server security, and digital certificates.

## IX. RISKS ASSOCIATED WITH INTERNET BANKING

### *A. Strategic Risk:*

On strategic risk Internet banking is relatively new and, as a result, there can be the absence of understanding among senior management about Internet banking potential and implications. Now the people having a strong technology backbone and don't have the knowledge of banking skill can take the initiative to deal with the system. E-initiatives can spring up in an incoherent and piecemeal manner in firms. They can be expensive and can fail to recoup their cost. Furthermore, they are often positioned as loss leaders (to capture market share), but may not attract the types of customers that banks want or expect and may have unexpected implications on existing business lines.

### *B. Business risks:*

Accepting Internet banking technology in bank, nobody knows much about the Internet banking technology. Internet banking customers will have different characteristics from the traditional banking customers no one can predict. In case of Internet banking, banks unable to assess the credit quality through Internet banking, banks may not achieve high credit quality as they do in face to face circumstances. It could be more difficult to assess the nature and quality of security offered at a distance, especially if it is located in an area of the bank is unfamiliar. Banks face three main types of operations at risk:

***a.*** ***Volume forecasts–*** It means accurate customer volume those are using Internet banking. It is very difficult for a bank to predict. Numerous banks doing their business online hence it is very difficult for banks in the Internet environment predict and manage the volume of customers that they will obtain. Various banks are unable to judge the exact volume of customer and exact demand it may suffer reputation and financial damage, and even compromises in security if extra systems that are inadequately configured or tested are brought on-line to deal with the capacity problems. For assessing strategic risk bank understands the market situation to undertake market research. Adopt systems with adequate capacity and scalability, do advertise campaigns of students. The bank should develop a business plan for adequacy in staff and handling technology securely.

***b.*** ***Management information systems*** - Numerous banks have not addressed management information issues. Hence, banks have difficulties to obtain adequate management information to monitor banking e-services. It can be notoriously difficult to establish new systems to ensure that sufficient, meaningful and clear information is generated and it is useful for handling of Internet banking transaction. Such information is particularly important in a new field like Internet banking. Banks are being encouraged by the FSA to make sure that management has all the information that they require in a format that they understand and that does not cloud the fundamental information with superfluous details.

***c.*** ***Outsourcing*** -The banks are using outsourcing as a medium for Internet banking services, security. The foremost cause of outsourcing is the cost reduction and bank does not have expertise in house to develop technology. Banks offering Internet banking services outsource related business functions, e.g. Security, either for reasons of cost reduction or, as is often the case in this field, because they do not have the relevant expertise in-house. Outsourcing a significant function can create material risks by potentially reducing a bank's control over that function.

### *C. Credit Risk:*

Internet banking service is popular in the world. It provides fast service and enables the customer to supply credit anywhere in the world. However, it is very difficult to look for identifying the customer and maintain security agreements to identify authorized users. When a transaction performs on different country and states, then it is difficult to which country's (or state's) jurisdiction applies to the transaction. Hence this is the risk to earnings or capital from a customer's failure to meet his financial obligations.

### *D. Liquidity Risk:*

Liquidity risk is the risk arising from a bank's inability to meet its obligations when they come due, without incurring unacceptable losses, although the bank may ultimately be able to meet itsresponsibilities. Liquidity risk may be significant for banks that specialize in electronic money activities if they are unable to guarantee that funds are adequate to cover redemption and settlement demands at any particular time. In addition, failure to meet redemption demands in a timely manner could result in legal action against the institution, and lead to reputations damage.

### *E. Security Risks:*

The security problem is the foremost issue for everyone both inside and outside the banking industry. Hence bank needs to provide proper security aids through which provide secure transaction for the customer and make a risk free environment. Banks take initiative to identify threats for that they need to be explicit in monitoring and managing the security threat. Securities threats arise are the unauthorized access of confidential or financial information, denial of services, crashing of websites, flaws in system design. All of these threats are very serious financial, legal and reputations implications.

Various banks observe hundreds of weaknesses. Most of the banks used “burglar alarms” to identify the unauthorized access of the system, which breaks the working of the system. The Bank should create a highly secure environment for the systems used high value, payments or those storing highly confidential information. The bank requires maintaining high security in inside and outside the bank area to protect the bank customer from financial loss or unauthorized access of high value system via the bank's internal network.

### *F. Reputational Risks:*

This is the risk arises due to adverse public opinion towards Internet banking services provided by the bank to the customer. Bank's reputation can be damaged due to limited availability, buggy software, and poor response of Internet banking services observed by the customer.

### *G. Legal Risk:*

Legal risk is the risk arises when the bank does not comply with the rules and regulations of other countries in Internet banking & virtual banking transaction.

## X. RISK MANAGEMENT PRINCIPAL

Risk management is important to maintain customer satisfaction, warding off the attackers, ensuring regulatory compliance, and improving shareholder value. In practice, however, technology risk management is too often a disjointed effort. It's especially challenging in large organizations, where separate regional offices or business units are likely to operate in silos, forging separate and uncoordinated paths to risk management, and often relying on patchwork efforts and quick fixes [15].

Following are the different risk management principals.

### *A. Board and Management Oversight:*

The Board of Directors and senior management should develop strong management and establish effective management oversight, against the risk found in e-banking activities, including the establishment of specific accountability, policies and controls to manage these risks.

a. The Board of Directors and senior management should take a review of Internet banking security and approved the bank's security control process
b. The Board of Directors and senior management should develop broad and establish a comprehensive and enduring due diligence and take an oversight process for managing the bank's outsourcing relationships.

### *B. Security Control:*

a. Banks should define appropriate measures to find out unauthorized access and also take care of banking transactions which are only performed by authorized user to conduct business over the Internet.
b. Banks should use transaction authentication methods that promote non- repudiation and establish accountability for e-banking transactions.
c. Banks should define appropriate measures to adopt adequate segregation of duties in e-banking systems, databases and applications.
d. Banks should define proper authorization controls and access privileges to access e-banking systems, databases and applications.
e. Banks should define appropriate measures to protect the data integrity of e-banking transactions, records and information.
f. Banks should define the appropriate audit trails for all e-banking transactions.
g. Banks should apply appropriate measures to achieve confidentiality of e-banking transactions when sensitive information transferred through the network and stored in the database.

### *C. Legal and Reputational Risk Management:*

a. The bank should take care of adequate information which is available on the banks' websites through that customer identifies the status and position of banks in the market to perform e-banking transactions.
b. Banks should define appropriate measures to assure loyalty to customer privacy requirements applicable to

the jurisdictions to which the bank is providing e-banking products and services.

c. Banks should provide operational capacity, business continuity and contingency planning processes which help to ensure the availability of e-banking systems and services.

d. Banks should develop appropriate plans for the incident which are happening response plans to manage, control and minimize problems arising from unexpected events.

## XI. RISK MANAGEMENT METHODOLOGY

Risk is arisen in commercial activity and banking is no exception to this rule. Now a day's global competition, increasing deregulation, introduction of innovative products and delivery channels has pushed risk management technology into the forefront of today's financial landscape.

Ability to determine the risks and find out appropriate remedies is the key to success in banking technology. It can be said that risk takers will survive.Generally in the banking environment, banks have been dealt with credit or default risk. For the perfect market economy, we have to deal with a market related risks like exchange risks, interest rate risk, etc. Operational risk, which had always existed in the system, would become more pronounced in the coming days as we have technology as a new factor in today's banks. The expansion in e-banking will lead to continuous awareness revisions of rules and regulate.

In future aspect, the Bank needs to develop a proper risk management structure for the future betterment. Banks understand the technology and related risk in assessing technology and strengthen technology based risk management tools. Following are the risk management techniques used by the bank for proper betterment.

### *A. Risk assessment:*

Risk assessment is the first phase in risk assessment methodology. In this method organization, find out how much percentage risk associated without side and insider threat to the Internet banking system. This will help with the organization to identify the appropriate method to control and reduce the existing risk. During risk assessments following steps are performed.

a. System characterization firstly, determines the scope of the system. IT system defines the bank consists of two main components. The first component is the IT systems which concentrate on Hardware, software, connectivity, operating personnel used by the system and second component is the operating environment which contains functional and technical requirements of the systems, security policies and level of protection towards data and network topologies used by the system.

b. Threat identification system depicts the goal to identify inside and outside threats created in Internet banking system and find out sources through which threats created in IT systems. Due to these threats identification side by side drawbacks of IT systems has also been identified which helps to find out possible solutions will require to control unauthorized access to the system.

c. The vulnerability identification checklist is prepared for identifying the weaknesses in the system that may develop distinct threat sources. Test the performance of existing systems, apply different security testing techniques and through that improve security plans require to apply on possible threats. Also prepares the checklist of required security remedies.

d. Control analysis analyses the controls that have been implemented in order to minimize or removed threats identified in previous steps.

e. The likelihood determination method bank monitors the identified threats and determines the overall probability of potential weaknesses found within a defined time period to take a regular review of the associated threat environment.

f. Impact analysis and risk determination measures, levels of risk to the IT system. It is used to measure the adverse impact of successful threat exercise of defects. Before beginning the impact analysis, banks need to know the detail knowledge about the process performed by the IT system and data sensitivity. System importance of bank for transactions performed through the system.

g. Control Recommendations step is an essential phase in risk assessment method. During this phase different controlling remedies are applied in identifying risk and eliminate the identified risk to create a climate in the organization to perform a powerful transaction. The goal of this phase aims to reduce the level of risk to the IT system and its data to an acceptable level.

h. Results Documentation is an important part during risk assessment. Once the assessment process has been carried out, then the available threat-sources, identified weaknesses. Type of risks accessed and recommended controls applied on theseaccessed risk have been stored in a proper format. Whatever results find out should be documented in an official report or briefing

### *B. Risk management:*

It starts with a clear understanding of the bank's risk assessment structure and identifying high-level risk exposures. After completion of the risk assessment process, from the defined risk appetite and identified risk exposure, strategies for managing risk can be set and responsibilities clarified to every consultant personally. Dependent on the type of risk observed and its impact on business, the board and senior management may choose to take up any of the three actions:

***a)*** ***Mitigate-*** for protecting the IT infrastructure Bank implements to acquire and deploy security technology controls.

***b)*** ***Transfer*** - share risk with partners or transfer to insurance coverage.

***c)*** ***Accept*** - formally acknowledge that the risk exists and monitor it.

At an elementary level, the first step is to do the risk assessment and that analyze the risk even if there is no immediate action to be taken by the system. For the effective enterprise risk management technique, the awareness of risk will control tactical decisions and IT framework. It should maintain a risk register in the form of a table called as a risk log that assists risk management.

Risk management uses risk logging to identify, analyze and manage risks in a clear and summarizing manner. It contains information of each identified risk. It records the action taken by the organization to solve problems arises during transaction execution. Record the analysis and evaluation of risks that have been identified. The register or the log may be made for a new project or investment.

a. Bank management needs to assess IT risks and apply security controls to manage risk
b. Bank management takes a review of IT-related risks, takes a periodic review, updating the database as per the need arises and applies security controls to solve the problems.
c. Bank's risk management considers all e-banking activities and integrated into its overall risk management approach. Effective management oversight is considered with e-banking activities, including specific accountability, policies and controls to manage all risks.
d. Appropriate incident response plans are prepared to control IT related risks which include communication strategies, assuring business continuity. Control reputation risk and limit liability associated with disruptions in their IT-enabled services, including those originating from outsourced systems and operations.
e. Operational risk is accessed and related controls are implemented and monitored
f. Appropriate measures are implemented to ensure adherence to customer privacy requirements applicable to the jurisdictions to which the bank is providing e-banking products and services, including foreign jurisdictions where the bank operates.
g. Appropriate procedures are implemented for developing software contracts between the organization and bank. Information security policy is designed by the organization when actual implementation is started. The centralized change control system is implemented at project or application levels so that changes are appropriately reviewed and approved under management of Internet banking project appropriate program and project management framework is implemented correct prioritization and coordination between projects. For major projects, formal project risk assessment needs to be carried out and managed on an ongoing basis.

### *C. Security policies and measures:*

Security is the combination of systems, applications, and internal controls employed to achieve the integrity, authenticity, and confidentiality of data and operating processes. Security of Internet banking depends on adequate security policies and security measures for processes within the bank, and for communication between the bank and external parties. Security policies and measures can limit the risk of external and internal attacks on electronic banking and electronic money systems, as well as reputation risk arising from security breaches.

Security policies are the guideline and responsibilities provided by the banks to the customer as well as employees of the banks for designing, implementing, and enforcing information security measures, and it may establish procedures to evaluate policy compliance, enforce disciplinary measures, and report security violations.

Security measures are combinations of hardware and software tools. Senior management mainly concentrates on the internal, external attacks, and misuse of electronic banking and electronic money. Such security measures include, encryption, passwords, firewalls, virus controls, and employee screening. Encryption uses cryptographic algorithms to encode plain text data into cipher text to prevent unauthorized observation. Passwords, pass phrases, personal identification numbers, hardware-based tokens, and biometrics are techniques for controlling access and identifying users.

Firewalls are combinations of hardware and software which will check the exterior access of unauthorized person to internal systems which will connect to the Internet. Firewall technology, if properly designed and implemented, it will be the prevailing tool for controlling unauthorized access to achieve data confidentiality and integrity. This technology is complex to design and can be costly. A well-planned design consists of enterprise-wide security requirements, detail information about the step by step procedures for performing operations, separation of duties, and selection of trusted personnel who are under the responsibility of the configuration and operation of the firewall. With the help of firewall, virus infected programs are sometimes difficult to find out. Hence management requires improving the prevention and detection controls to reduce the chances of virus attack and data destruction. Also include network controls, end-user policies, user training, and virus detection software.

### *D. Internal communications:*

Operational, reputations, legal, and other risks can be managed and controlled by the bank itself. Senior management communicates with staff regarding the precautions of electronic banking and electronic money is intended to support the overall goals of the bank. At the same time, technical staff should clearly communicate with the senior management, how systems are to be used to work, as well as the strengths and weaknesses of the systems. Such procedures can reduce operational risks of inadequate systems design, including incompatibility of different systems within a banking organization; data integrity problems, reputation risk associating with customer dissatisfaction that systems did not work as expected, credit and liquidity risk. For performing sufficient internal communication bank needs to provide all policies and procedures in writing to the worker. Senior management provides on-going education, upgrading skills and knowledge of contemporary technological progress to avoid operational risk arises from lack of staff and management expertise.

### *E. Evaluating and upgrading:*

Evaluating products and services before they are implemented on a widespread basis can also help to reduce operational and reputation risks. Before launching any product system needs to conduct tests to check the system performance and find out the system can perform the functions properly.Review the capabilities of existing hardware and software regularly.

### *F. Disclosures and customer education:*

Disclosures and customer education may help a bank to control legal and reputation risk. Because consumers can understand the bank's policies, the new technology and how to use new products and services, fees charged for services and products, problem and error resolution procedures. This will help the bank to fulfil the consumer protection, privacy laws and regulations.

### *G. Contingency planning:*

A bank can limit the risk of disruptions in internal processes or in service or product delivery by developing contingency plans that establish its course of action in the event of a disruption in its provision of electronic banking and electronic money services. The contingency plan may address data recovery, complementary data-processing capabilities, emergency staffing, and customer service support. Banks should ensure that their contingency operations are as sheltered as their normal production operations. On the Internet banking bank mainly depend on the hardware vendor, software provider, Internet providers. Bank management may insist that such service providers have backup capabilities. In addition, management may also define in the agreement if above mentioned providers are not providing sufficient information then compensating actions should be taken on them.

Contingency planning helps banks to control reputation risk are arising from the bank's own actions or problems experienced by another institution offering the same or similar Internet banking service. For example, banks may wish to establish procedures to address customer problems during system disruptions.

### *H. Monitoring risks:*

Monitoring is the decisive aspect found in the risk management process. Monitoring is an important part of any risk management process. Currently, technology can change rapidly when innovations are required. In monitoring phase system testing and auditing can be performed.

### *I. System testing and system inspection:*

In Internet banking system testing helps to identified system problems, disruptions, and attacks. In testing phase find out the internal, external threats of the system. In system inspection monitor the exact problem, anomalies, and on-going judgments regarding the effectiveness of security through routine operations.

### *J. Auditing:*

Auditing can provide independent control mechanism for detecting deficiencies and minimizing internal and external risks of Internet banking services. The role of the auditor is to put in place standard policies and procedures for dealing with Internet banking services. The important thing is that those people’s doing the audit is fully skilled personnel such as a computer security consultant or other professional with relevant expertise is necessary.

### *K. Management of cross border risks:*

Management of cross border risks may be more complex than risks banks face within their home country. Hence, banks give attention towards to appraise, controlling, and monitoring operation, reputation, legal and other risks arising from cross border electronic banking and electronic money activities. Banks that choose to provide services to customers in different nationalized markets will need to understand different national legal requirements. Develop an appreciation for national differences in consumer expectations and knowledge of products and services. In addition, senior management should ensure that existing systems for credit extension and liquidity management take into account potential difficulties arising from cross border activities. A bank may need to assess country risk and promote contingency plans that take into account service disruptions due to problems in the economic or political climate abroad. A bank may also face difficulties in enforcing the fulfilment of a Foreign Service provider’s responsibility. In the case of banks relying on service providers located abroad, national supervisors may want to assess the accessibility of information from, and consider the activities of, cross-border service providers on a case-by-case basis.

Federal supervisors can play a significant role in identifying and discussing jurisdictional ambiguities. They can also continue efforts to promote measures to detect unsafe and illegal practices. Finally, national supervisors can continue, and strengthen, cooperative efforts to give information on product and service innovations and industry practices.By tackling customers’ security concerns, authorities may encourage a larger number of consumers to use this delivery channel, which would allow Internet banks to capture more of the potential scale efficiencies implied in our estimations [16].

Predictable communication security measures through authentication like OTP and encryption using SSL are no longer satisfactory countermeasures for all transactions of online banking. Banks, who apply for the AhnLab Online Security Service (AOS), the AhnLab Online Security Service in their online banking system will be highly competitive in attracting customers because they are offering an outstanding security service that outperforms those of other banks. Banks the AOS can minimize the fraud loss by preventing the incidence of cybercrimes well in advance [17].

## XII. CONCLUSION

The proficient flow of information about the customer is the heart of the financial service industry. In order to protect consumers, banking industry required to provide privacy and security during financial transactions. In the recent past, the Indian banking sector fully concentrates on developments and investments. In this sector, there are enormousopportunity and several challenges. Threats in financial transaction are increased nowadays. It is very difficult for the banks to control these threats. To provide a secure Internet banking service bank need to do the assessment of security risks. Banks need to expand and put into practiceefficientstrategy and procedural skeleton to guide these risks. For management of Internet banking risk bank need to take an initiative to raise customer orientation by educating them about new technology and security issues. Continuing with next chapter entitled as ‘Data analysis and Interpretation’.

## XIII. REFERENCES

[1]. Tero Pikkarainen, K. P. Consumer acceptance of online banking: an extension of the technology acceptance model. Internet Research, 14 (3), 224-235.

[2]. Heikki Karjaluoto, M. M. (2002). Factors underlying attitude formation towards online banking in Finland. International Journal of Bank Marketing, 20 (6), 261-272.

[3]. www. shodhganga.inflibnet.ac.in

[4]. Mirani, R. S. (2011). Designing a model for analyzing the effect of risks on ebanking adoption by customers: A focus on developing countries. African Journal of Business Management, 5 (16), 6684-6697.

[5]. www.soopertutorials.com/technology/disaster-recovery/1590-risk-assessment-of-e-banking.html). (Accessed on 09/07/2013 at 4:13 pm)

[6]. (April 2012). Indian Banking Industry

[7]. http://researchreport4u.blogspot.com/2012/03/uses-of-Internet-banking-services.html.(Accessed on 12/09/2013 at 4:30 pm)

[8]. "Electronic payment systems(EPS)." http://repository.ust.hk/dspace/bitstream/1783.1/1859/1/eps.pdf.

[9]. www. slideshare.net. (Accessed on 10/12/2013 at 7:30 pm)

[10]. http://www.rbi.org.in/scripts/PublicationReportDetails.aspx?ID=617. (Accessed on 15/12/2013 at 7:10 pm).

[11]. http://oreilly.com/catalog/crime/chapter/cri_02.html. ((Accessed on 11/02/2014 at 9:30 pm)

[12]. http://my.safaribooksonline.com/book/certification/cissp/9781118332108/chapter-1-access-control/toc1.(Accessed on 10/04/2014 at 7:40 pm)

[13]. Karen Furst, W. W. (September 2000). Internet Banking: Developments and Prospects. OCC Economics Working Paper 2000-9 .

[14]. http://www.slideshare.net/hcc79/online-security-encryption. (Accessed on 13/02/2013 at 1:40 pm)

[15]. Managing FSI technology risk Use HP Software for technology risk management Business white paper.

[16]. Javier Delgado, I. H. (2007). Do European Primarily Internet Banks Show Scale and Experience. European Financial Management, 13 (4), 643-671.

[17]. Online Banking:Threats and Countermeasures. (June, 2010). AhnLab, Inc.

## Short Bio Data for the Author

Prof. Minakshi Dattatraya Bhosale. Working as a head of faculty of MCA, Yashoda technical campus Satara, Maharashtra, India. Completed MCA with first rank in Shivaji University and register for the PhD in Shivaji University Kolhapur. She was having 13 years teaching experience and 2 years Industrial experience in reputed organisation. Published couple of research papers in national and international journals