ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 11, November 2016

A Critical Study of E-Banking: Their Risks and Mechanisms of Risk Management

Dr.Eknath Shankarrao Mundhe

Assistant Professor, Department of Economics, Karmaveer Bhaurao Patil College, Vashi, Navi Mumbai, Maharashtra, India

ABSTRACT: Nowadays, advances in information and communication technologies, has provided an opportunity for banks to provide their electronic services to their customers in remote areas. The evolution of electronic banking (e-Banking) started with the use of automatic teller machines (ATMs) and has included telephone banking, direct bill payment, electronic fund transfer and online banking. The development of e-banking services and e-commerce (including electronic money) can provide significant opportunities for banks. E- Banking may soon convert from a complementary to the main provider of financial services and products. Electronic banking is generally an extension of traditional banking, using the internet as an electric delivery channel for banking products and services. The banking today is redefined and re-engineered with the use of IT and it is sure that the future of banking will offer more sophisticated services to customers with the continuous product and process innovations. Application of information technology in banking brings, with one hand, strong organizational and economic growth potential, and on the other hand, opens space for the emergence of new forms of risk. So, rapid development potential of e-banking carries risks and benefits.

This research paper will introduce to e-banking, giving the meaning, functions, types, advantages, risks, limitations and their management of e-banking

KEYWORDS: e-banking, risks, risk management, electronic banking, challenges.

I. INTRODUCTION

While electronic banking in the form of automatic teller machines and telephone banking has been around for a number of years, the popularity of accesing banking services through the internet and mobile phones is rising. Increasingly, not only basic services are offered such as balance inquiry, funds transfer and bill payment-but also loan and credit card applications, foreign exchange transactions, new accounts as well as brokerage and insurance services. E-banking are changing and being improved because of the intense competition between the banks online. Banking industry must adapt to the electronics age, which in its turn is changing all the time.

Internet banking (or E-banking) means any user with a personal computer and a browser can get connected to his bank's website to perform any of the virtual banking functions. In internet banking system the bank has a centralized database that is web-enabled. All the services that the bank has permitted on the internet are displayed in menu. Once the branch offices of bank are interconnected through terrestrial or satellite links, there would be no physical identity for any branch. It would be a borderless entity permitting anytime, anywhere and anyhow banking.

Electronic banking can be defined as the use of electronic delivery channels for banking products and services and is a subset of electronic finance. The most important electronic delivery channels are the internet, wireless communication networks, automatic teller machines, and telephone banking. Internet banking is a subset of e-banking that is primarily carried out by means of the internet. The term transactional e-banking is also used to distinguish the use of banking services from the mere provision of information.

E-banking is a range of banking services that utilizes electronic equipment and includes Telephone banking, Net Banking, ATM, Debit/Credit Card. EFT, AFT etc. Many banks have modernized their services with the facilities of computer and electronic equipment's. The electronics revolution has made it possible to provide ease and flexibility in banking operations to the benefit of the customer. The e-banking has made the customer say good-bye to huge account registers and large paper bank accounts. The use of ATM's lead to the concept of 'anywhere' and 'anytime' banking.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 11, November 2016

Through the use of ATM cards, one can operate his bank account to withdraw money from any of the bank's ATM installed or available at the nearest site. Process of e-banking starts with opening the website and ends with making the payment.

Online banking was first introduced in the early 1980s in New York, United States. Four major banks — Citibank, Chase Manhattan, Chemical Bank and Manufacturers Hanover-offered home banking services. Chemical introduced its Pronto services for individuals and small businesses in 1983, which enabled individual and small-business clients to maintain electronic chequebook registers, see account balances, and transfer funds between checking and savings accounts. Pronto failed to attract enough customers to break even and was abandoned in 1989. Other banks had a similar experience.

Around 1994, banks saw the rising popularity of the internet as an opportunity to advertise their services. Initially, they used the internet as another brochure, without interaction with the customer. Early sites featured pictures of the bank's officers or buildings, and provided customers with maps of branches and ATM locations, phone numbers to call for further information and simple listings of products. In 1995, Wells Fargo was the first U.S. bank to add account services to its website, with other banks quickly following suit. That same year, Presidential became the first U.S. bank to open bank accounts over the internet. According to research by Online Banking Report, at the end of 1999 less than 0.4% of households in the U.S. were using online banking. At the beginning of 2004, some 33 million U.S. households (31%) were using some form of online banking. Five years later, 47% of Americans used online banking, according to a survey by Gartner Group. Meanwhile, in the UK online banking grew from 63% to 70% of internet users between 2011 and 2012.

At present, the personal e-bank system provides the inquiry about the information of account, card accounts' transfer, bank-securities accounts transfer, the transaction of foreign exchange' the b2c disbursement on net client service, account management, reporting the loss if the account etc.

II. RELATED WORK

To-day, we cannot think about the success of a banking system without information technology and communication. It has enlarged the role of banking sector in the economy. The financial transactions and payment can now be processed quickly and easily. The banks with the latest technology and techniques are more successful in the competitive financial market. They have been able to generate more and more business resulting in their greater profitability.

Dannenberg and Kellner (1998), in their study, overviewed the opportunities for effective utilization of the internet with regard to the banking industry. The authors evaluated that appropriate application of today's cutting edge technology could ensure the success of banks in the competitive market. They evaluated the services of banks via internet as websites provide sophisticated line of products and services at low price. The authors analyzed that transactions via internet reduce the risk of data loss to customers, chance to cut down expenses, higher flexibility for bank employees, re-shaping thebanks' image into an innovative and technologically leading institutes, etc. The researchers found that banks could move one step further by entering into a strategic alliance with internet service provider. So, the bank of tomorrow stands to be feasible with today's technology.

Suresh (2008), highlighted that recently developed e-banking technology had created unpredicted opportunities for the banks to organize their financial products, profits, service delivery and marketing. The objectives of the study were to evaluate the difference between traditional and e-banking, and to identify the core capabilities for the best use of e-banking. The author analyzed that e-banking will be an innovation if it preserved both business model and technology knowledge, and disruptive if it destroys both the model and knowledge. He also differentiated e-banking from traditional banking in five ways, namely, value proportion, market scope, cost structure, profit potential and value network. However, in order to exploit technical and business capabilities of e-banking, banks should generate more customers inside and outside India so that more revenues could be generated that lead to better future of Indian economy.

Chalam and Nageswara (2006) focused that as the computer touched each and every aspect of the economy, so banking sector was not an exception to it. The objective of the study was to find out change in banking sector through the techniques of e-banking. The authors evaluated several e-banking products like ATM, EFT, ECS, EDI, telebanking, etc. E-banking had benefited to the individual through anywhere, anytime banking; to traders and merchants through

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 11, November 2016

immediate settlement of payment; to banks through unlimited network, online banking, attracting and retaining the customers, debit and credit card facilities; and to the nation through globalization of trade, more exports, more transparency in business, etc. The researchers concluded that emerging challenge in e-banking was due to lack of awareness among people, no cyber laws by government and low density of telephone lines and low computerization of banking activities. They recommended that banks should adopt hardware and software security measures, appoint skilled personnel and adoption of digital signature certification authority so as to tackle the major challenges in e-banking.

Sarangapani and Mamatha (2008) explained the concept of e-banking and highlighted all the concerns and challenges while implementing the same. The authorsemphasized that e-banking was necessary not only for improving the quality of servicesrendered to the customers but also for better marketing of products. The authorsevaluated various e-banking modems for banking transactions like ATM, EFT, ECS,SPNS, PC banking, mobile banking and internet banking. But they mainly emphasizedon virtual banking, smart cards, e-cheques and internet banking. They analyzed thewebsites of various banks for internet banking adoption in which private sector bankswere providing maximum IB services followed by public sector banks, foreign banks andold private sector banks. The author suggested some measures which could contributetowards greater adoption of e-services. The customers should be taken into confidencethat the transactions made by them are risk free, and there is no scope of any fraud.Further, they should also be assured that hackers can do no harm to their interests.Furthermore, the system should be free from legal intricacies.

III. BENEFITS OF E-BANKING

***A. TO THE CUSTOMER*:**Anywhere Banking no matter wherever the customer is in the world. Balance enquiry, requestfor services, issuing instructions etc., from anywhere in the world is possible.Anytime Banking – Managing funds in real time and most importantly, 24 hours a day, 7days aweek according to convenience of the customers.Brings down 'Cost of Banking' to the customer over a period of time.Cash withdrawal from any branch / ATM.On-line purchase of goods and services includingonline payment for the same.

***B. TO THE BANK*:** Innovative, scheme, addresses competition and present the bank as technology driven in thebanking sector market.Reduces customer visits to the branch and thereby human intervention.Inter-branchreconciliation is immediate thereby reducing chances of fraud and misappropriation.On-line banking is an effective medium of promotion of various schemes of the bank, amarketing tool indeed. Integrated customer data paves way for individualized and customizedservices.

IV. RISKS IN E-BANKING

***A. OPERATIONAL RISK*:** Operations risk arises from fraud, processing errors, system disruptions, or other unanticipated events resulting in the institution's inability to deliver products or services. This risk exists in each product and service offered. The level of transaction risk is affected by the structure of the institution's processing environment, including the types of services offered and the complexity of the processes and supporting technology. In most instances, e-banking activities will increase the complexity of the institution's activities and the quantity of its operations risk, especially if the institution is offering innovative services that have not been standardized. Since customers expect e-banking services to be available 24 hours a day, 7 days a week, financial institutions should ensure their e-banking infrastructures contain sufficient capacity and redundancy to ensure reliable service availability. Banks face three main types of operations risk, 1.Volume Forecasts. 2. Management Information Systems. 3. Outsourcing.

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

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 11, November 2016

Internet environment which is a public domain and attempts at unauthorized access could emanate from any source and from anywhere in the world with or without criminal intent. Attackers could be hackers, unscrupulous vendors, disgruntled employees or even pure thrill seekers. In addition to external attacks banks are exposed to security risk from internal sources e.g. employee fraud. Employees being familiar with different systems and their weaknesses become potential security threats in a loosely controlled environment. They can manage to acquire the authentication data in order to access the customer accounts causing losses to the bank. Unless specifically protected, all data / information transfer over the Internet can be monitored or read by unauthorized persons. There are programs such as 'sniffers' which can be set up at web servers or other critical locations to collect data like account numbers, passwords, account and credit card numbers. Data privacy and confidentiality issues are relevant even when data is not being transferred over the net. Data residing in web servers or even banks‟ internal systems are susceptible to corruption if not properly isolated through firewalls from Internet. Proper access control and technological tools to ensure data integrity is of utmost importance to banks. Identity of the person making a request for a service or a transaction as a customer is crucial to legal validity of a transaction and is a source of risk to a bank. A computer connected to Internet is identified by its IP (Internet Protocol) address. There are methods available to masquerade one computer as another, commonly known as 'IP Spoofing'. Likewise user identity can be misrepresented. Hence, authentication control is an essential security step in any e-banking system. Non-repudiation involves creating a proof of communication between two parties; say the bank and its customer, which neither can deny later. Banks' system must be technologically equipped to handle these aspects which are potential sources of risk.

***C. SYSTEM ARCHITECTURE AND DESIGN RISK*:** Appropriate system architecture and control is an important factor in managing various Kinds of operational and security risks. A bank faces the risk that the systems it chooses are not well designed or implemented. For example, a bank is exposed to the risk of an interruption or slow-down of its existing systems if the electronic banking or electronic money system it chooses is not compatible with user requirements. Many banks are likely to rely on outside service providers and external experts to implement, operate, and support portions of their electronic money and electronic banking activities. Such reliance may be desirable because it allows a bank to outsource aspects of the provision of electronic banking and electronic money activities that it cannot provide economically itself. However, reliance on outsourcing exposes a bank to operational risks. Service providers may not have the requisite expertise to deliver services expected by the bank, or may fail to update their technology in a timely manner. A service provider's operations could be interrupted due to system breakdowns or financial difficulties, jeopardizing a bank's ability to deliver products or services. The rapid pace of change that characterizes information technology presents banks with the risk of systems obsolescence. For example, computer software that facilitates the use of electronic banking and electronic money products by customers will require updating, but channels for distributing software updates pose risks for banks in that criminal or malicious individuals could intercept and modify the software. In addition, rapid technological change can mean that staff may fail to understand fully the nature of new technology employed by the bank. This could result in operational problems with new or updated systems.

***D. REPUTATIONAL RISK*:** Reputational risk is the risk of getting significant negative public opinion, which may result in a critical loss of funding or customers. Such risks arise from actions which cause major loss of the public confidence in the banks' ability to perform critical functions or impair bank customer relationship. It may be due to banks‟ own action or due to third party action. The main reasons for this risk may be system or product not working to the expectations of the customers, significant system deficiencies, significant security breach (both due to internal and external attack), inadequate information to customers about product use and problem resolution procedures, significant problems with communication networks that impair customers' access to their funds or account information especially if there are no alternative means of account access. Such situation may cause customer-discontinuing use of product or the service. Directly affected customers may leave the bank and others may follow if the problem is publicized. Other reasons include losses to similar institution offering same type of services causing customer to view other banks also with suspicion, targeted attacks on a bank like hacker spreading inaccurate information about bank products, a virus disturbing bank's system causing system and data integrity problems etc. Possible measures to avoid this risk are to test the system before implementation, backup facilities, contingency plans including plans to address customer problems during system disruptions, deploying virus checking, deployment of ethical hackers for plugging the loopholes and

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 11, November 2016

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

***E. LEGAL/COMPLIANCE RISK*:** Legal risk is the risk of non-compliance with legal or regulatory requirements. The legal risks are directly related to the electronic banking and they are increased as its use is extended. They mainly stem from the uncertainty that exists in the legal – regulative framework concerning the electronic banking. In most countries an explicit regulating framework does not exist and this is owed to the little experience regarding the sector of electronic banking. The problem becomes even bigger when a bank offers its electronic services to other countries as well, since a unified legal frame in international level does not exist. Each country puts its own rules into effect and it is difficult for a bank to constantly adapt its services and to be acquainted with all the laws that are in effect in every country. Another legal risk is related with the protection of the customers' personal data. Bad use by the bank personnel or by exterior malignant intruders can expose a bank in serious legal risks. It is possible that the intruders acquire access in the databases of the banks and use the data of customers in order to commit a fraud. In this case a legal risk is created by the bad or not certified use of customers‟ data. The legal risks, in which the financial institutions will be exposed from the use of electronic banking, are expected to increase because of the uncertainty that characterizes the wider legal framework and the specific lawful regulations of transactions through an open electronic network as the internet is. The uncertainty with regard to the validity of transactions, the protection of personal data, the involuntary consumer's exposure to foreign jurisdiction, the tax evasion, the laundering of money, the electronic fraud but also the legal responsibility in case a system collapses, increase the exposure to the legal regulatory risks. In terms of the European Union, a regulating frame has been developed that is concerned with questions such as the electronic (digital) signatures, the distant rendering of financial services, as well as the Directive on the electronic commerce. A customer inadequately informed about his rights and obligations, may not take proper precautions in using Internet banking products or services, leading to disputed transactions, unwanted suits against the bank or other regulatory sanctions. In the enthusiasm of enhancing customer service, bank may link their Internet site to other sites also. This may cause legal risk. Further, a hacker may use the linked site to defraud a bank customer. Compliance and legal issues arise out of the rapid growth in usage of e-banking and the differences between electronic and paper-based processes. E-banking is a new delivery channel where the laws and rules governing the electronic delivery of certain financial institution products or services may be ambiguous or still evolving. Specific regulatory and legal challenges include: Laws and regulations governing consumer transactions require specific types of disclosures, notices, or record keeping requirements. These requirements also apply to e-banking, and Reserve Bank of India continues to update consumer laws and regulations to reflect the impact of e-banking and on-line customer relationships. Some of the legal requirements and regulatory guidance that frequently apply to e-banking products and services have been issued by R.B.I. in its notification on 14th June, 2001, which were the findings of a working group on Internet Banking. These guidelines are available on the web site of RBI.

***F. MONEY LAUNDERING RISK*:** Money laundering is the practice of engaging in financial transactions in order to conceal the identity, source, and/or destination of money, and is a main operation of the underground economy. Money laundering is called what it is because that perfectly describes what takes place - illegal, or dirty, money is put through a cycle of transactions, or washed, so that it comes out the other end as legal, or clean, money. In other words, the source of illegally obtained funds is obscured through a succession of transfers and deals in order that those same funds can eventually be made to appear as legitimate income. Every financial institution is charged with the responsibility of developing policies and procedures to combat money laundering, which includes the duty to be aware of trends and adaptations in the methods by which money laundering is carried out. The most difficult aspect of this responsibility is a financial organization's ability to anticipate new criminal behaviour and to proactively implement protocols before the criminal behaviour occurs. As Internet banking transactions are conducted remotely banks may find it difficult to apply traditional method for detecting and preventing undesirable criminal activities. Application of money laundering rules may also be inappropriate for some forms of electronic payments. Thus banks expose themselves to the money laundering risk. This may result in legal sanctions for non-compliance with "know your customer" laws. To avoid this, banks need to design proper customer identification and screening techniques, develop audit trails, and conduct

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 11, November 2016

periodic compliance reviews, frame policies and procedures to spot and report suspicious activities in Internet transactions.

***G. STRATEGIC RISK*:** On strategic risk E-banking is relatively new and, as a result, there can be a lack of understanding among senior management about its potential and implications. People with technological, but not banking, skills can end up driving the initiatives. 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. Banks should respond to these risks by having a clear strategy driven from the top and should ensure that this strategy takes account of the effects of e-banking, wherever relevant. Such a strategy should be clearly disseminated across the business, and supported by a clear business plan with an effective means of monitoring performance against it. Poor e-banking planning and investment decisions can increase a financial institution's strategic risk. Early adopters of new e-banking services can establish themselves as innovators who anticipate the needs of their customers, but may do so by incurring higher costs and increased complexity in their operations. Conversely, late adopters may be able to avoid the higher expense and added complexity, but do so at the risk of not meeting customer demand for additional products and services.

V. MACHANISM OF E-BANKING RISK MANAGEMENT

For an increasing number of banks there may be a strategic reason for engaging in electronic banking and electronic money activities. In addition, greater use of electronic banking and electronic money may increase the efficiency of the banking and payment system, benefiting consumers and merchants. At the same time, there are risks for banks engaging in electronic banking and electronic money activities. Risks must be balanced against benefits; banks must be able to manage and control risks and absorb any related losses if necessary. The rapid pace of technological innovation is likely to change the nature and scope of risks banks face in electronic money and electronic banking. Supervisors expect banks to have processes that enable bank management to respond to current risks, and to adjust to new risks. A risk management process that includes the three basic elements of assessing risks, controlling risk exposure, and monitoring risks will help banks and supervisors attain these goals. Banks may employ such a process when committing to new electronic banking and electronic money activities, and as they evaluate existing commitments to these activities.

Scammers and thieves are out there, but you can protect yourself. Infamous bank robber Willie Sutton, when asked why banks were his favourite target, responded, "Because that's where the money is. The modern-day Willie Suttons of the world target bank Web sites for the same reason. With online transactions, money is represented in the form of electronic records of ownership, which means online bank robbers can steal more money, in less time, than by stealing literal currency--and they don't even need a getaway car. But that doesn't mean online banking necessarily has to be a riskier proposition. "Internet banking is terribly secure," says Brad Adrian, an Internet banking analyst with Gartner. "Financial services providers...make their systems as secure as possible." But, he says, "unscrupulous people using phishing, keystroke collection, or similar activities" to steal your passwords or account numbers are a growing problem.

GOING PHISHING: Phishing scams, in which attackers use spoof e-mails and Web sites to lure users into entering personal financial information (such as credit card numbers, bank account information, and passwords), have increased in the last several months. Yet even though public awareness of these scams has grown, people continue to fall victim to them in increasing numbers. The click-through rate on phishing e-mails is 3 percent, estimates AvivahLitan, vice president and research director at Gartner. That compares with a response rate of about 0.5 percent for spam, he says. One possible reason for this: People take e-mail from their bank very seriously, he says. In part the solution is better customer education, he adds, but banks could also do more to prevent the scams from working in the first place. Online criminals-including those who phish for a living--have become even more sophisticated, creating fraudulent Web sites and e-mail messages that are harder to detect. Professional phishing criminals even work current events into their attacks to make them seem more realistic: One recent scam, for example, posed as an e-mail soliciting campaign donation.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 11, November 2016

PROTECT YOURSELF: Log on to banks only from a secure computer. Never log on from a public computer in a hotel or cafe, and be careful when logging on to unknown networks with a laptop. If you get a warning e-mail, call your bank - don't click on any provided links. If your computer is acting strangely - for instance, reacting slowly or getting popups - avoid using it for online banking until you can get it checked out. Keep anti-virus and anti-spyware software up to date. Install and maintain a firewall. Never respond to any e-mail that requests personal information. Be leery of fly-by-night, Internet-only banks with high interest rates on savings or checking accounts. Make sure the bank is FDIC-certified and is insured. And, use a different user name andpassword for each financial account. The password should be complex, with numbers and symbols, and changed regularly.

VI.CONCLUSION

No doubt, internet facility makes banking easy and expanding to the masses. However, it having their inherent risks due to its nature, legal framework system, hackers interfere and frauds etc. In order to overcome these issues there is urgent need of consistence legal framework, strong implementing and responsible legal controlling authority which should be able to provide risk free conducive environment for having more banking services to the customers by using e- banking . If banking system provides confidence to the customers, definitely it will help to enter in new era of development of banking by e- banking.

REFERENCES

[1] Malhotra, P. and Singh, B. "The impact of internet banking on bank's performance: the Indian experience", South Asian Journal of Management, Vol. 13, No. 4, 2006.
[2] Prof. Virender Singh Solanki, "risks in e-banking and their management" international journal of marketing, financial services & management research vol.1 issue 9, September 2012.
[3] Ravi, V., Mahil, C. and VidyaSagar, N. "Profiling of internet banking users in India using intelligent techniques", Journal of Services Research, Vol. 6, No. 2, October 2006.
[4] Ganesan R, and Vivekanandan K, "A secured hybrid architecture model for internet banking (e-banking)". Journal of Internet banking and commerce, vol.14, no.1, 2009.
[5] Agarwal, N., Agarwal, R., Sharma, P. and Sherry, A. M., "E banking for comprehensive E Democracy: An Indian Discernment", Journal of Internet Banking and Commerce, Vol. 8, No. 1, June, 2003.
[6] Hawke J.D. "Internet Banking- Challenges for banks and regulators", Banking in the new millennium, iup, p 16, 2004.
[7] Iyer A. "Banks sharing Tech Infrastructure", p9, The Economic times,September 21st, 2006.
[8] Basel Committee, (2003). Risk management for E-Banking. Available: http:// www.bis.org.
[9] Beckett, A., Hewer, P., &Howcroft, B. "An exposition of consumer behaviour in the financial services industry." The International Journal of Bank Marketing, 18(1). 2000.
[10] FFIEC Information Technology Examination Handbook,Management booklet, Risk Overview".[online]. <http://www.ffiec.gov/ffiecinfobase/booklets/mang/02.html > [July 2008]
[11] Data Protection in Consumer E-banking Journal of Internet Banking and Commerce, vol.11,no.1, April 2006, (http://www.arraydev.com/commerce/jibc/)
[12] Nair .K.G.K and Prasad P.N, Development through Information Technology in Developing Countries: Experiences from an Indian State, The Electronic Journal of Information Systems in Developing Countries, 2002.
[13] De Young, R., "The Performance of Internet-based Business Models: Evidencefrom the Banking Industry", Journal of Business, Vol. 78 No. 3, pp. 893-94, 2005.
[14] Uppal, R.K. and Jatana, Rimpi - Indian banking moving towards information technology. New Delhi : Mahamaya,254p, 2008.
[15] Vageesh, N.S.- — New private banks : new kids on the Blockl, Business line, March 2000.