CHAPTER 2

REVIEW

OF

LITERATURE
CHAPTER 2

REVIEW OF LITERATURE

2.1 Introduction:

Literature review is one of the most important phases in research work. The literature review helps to define the research gap. The main aim of literature review is to identify the current issues. Information Technology (IT) is very powerful in today’s world, and financial institutions are the backbone of the Indian economy. Today Indian banking industry is in the middle of an IT revolution. All the nationalized banks and majority of the cooperative banks in India are going for core banking solutions. The application of IT in Banks has reduced the scope of traditional or conventional banking with manual operations. Nowadays banks have moved from disbursed to a centralized environment, which shows the impact of information technology on banks. Banks are using new tools and techniques to find out their customer needs and offer them tailor made products and services. The impact of automation in banking sector is difficult to measure. The primary search strategy was used to find the data relevant to the research gap/ research questions. It includes journals, online databases, Ph. D thesis from various universities, books etc. The sources for the primary search are listed below:

- INFLIBNET (Information and Library Network Centre)
- IEEE explore
- Reserve Bank of India website
- ScienceDirect (scientific database journal)
- IDBRT (Institute for Development and Research in Banking Technology)
- Google scholar (scholar.google.com)
- NIST Online publication
- Urban cooperative banks annual reports

The sphere of the research study is mainly linked with information security in CORE banking, security standards and urban cooperative banks. Therefore the researcher has reviewed the literature focusing on these domains of the study. The literatures available to the researcher on the application of information security in Indian banks are classified according to the related topics as mentioned below:
1. Ph.D. theses submitted to various universities

2. Research papers and articles published in proceedings, journals and periodicals on:
   a) Cooperative banking and Information Technology
   b) Information Technology in Banking a global perspective
   c) Online banking security issues : Global Scenario
   d) Information Security
   e) Information Security Standards
   f) Various articles published in news papers on information security

2.2 Ph.D. Thesis from various universities:
The number of research students has studied the various aspects of the urban cooperative banks (UCBs) for their research study at Ph. D. level. These references are as listed below:

2.2.1 Study of various aspect of urban cooperative banks
1. Mr. Shouche Vilas G. (1996)[1] had carried out the research work on “A study of Management of Funds of Selected Urban Co-operative Banks in Maharashtra”. In his thesis the research found that, in Maharashtra the first urban co-operative bank is registered in Pune named “Deference Accounts Co-operative Bank Ltd” on 9th January 1906. The second urban co-operative banks are also registered in Pune named as “Cosmos urban co-operative bank Ltd.” on 18th January 1906. The third urban co-operative bank registered in Barshi, Dist. Solapur name as “The Barshi Central Urban Co-operative Bank Ltd” on 29th April 1906.

In his study the researcher observed that after the enactment of Cooperative Society Act 1912, the number of cooperatives bank were established but the growth of urban cooperative bank were took place only after the second World War.

2. Mr. Zadesh Hessam Hedayat (1993)[2] in his research work author suggested that the cooperative movement in Maharashtra provides a model to the country in respect of qualitative and quantitative aspects. Researcher found that Maharashtra is leading in urban co-operative banks as compared to other states in the country. The urban co-operative banks in Maharashtra compete with commercial banks and they are also able to attract more customers.

3. Mr. P.S. Sahasrabudhe (1993)[3] has studied a role of urban co-operative bank in Maharashtra state. The researcher found in his study that there is interstate imbalance in the development of urban co-operative banks in Maharashtra. The urban co-operative banks in Maharashtra had significant growth rate of deposit mobilization, as the annual rise in the deposit was about 20 to 22 percent. In the study researcher observed that many of the older banks do not satisfy certain viability norms laid down by Reserves Bank of India. Researcher also observed that most of the urban co-operative banks are earning profits.

4. Mr. Rainch R.N (1992)[4] had carried out a research for Ph.D. entitled “Co-operative study of Personnel Policies and Practices in Commercial Banks and Co-operative banks in Satara City”. In his study the researcher observed that:
   - The S.T. Co-operative Bank Ltd, Mumbai is formed with the main purpose of providing loans and advances to the employee of the state road transport corporation.
   - The branch manager is solely responsible for executive administration and day to day functioning at the branch level.

The bank accepts various types of deposit from member as well as non-member, but lending operations are restricted to its member only.

5. **Aziz Gord (2006)**[5], carried out research on ‘A Study Of Audit Of Banks in Electronic Data Processing (EDP) Environment With Reference To Some Selected Islamic Banks In Middle East (1990-2004)”. In his study researcher has explained the necessity of existence of banks and their services to the society. The study focused its emphasis on the audit of banks in Electronic Data Processing (EDP) system and search about usefulness of new auditing techniques namely Computer-Assisted Audit Techniques (CAATs), In addition to the manual audit techniques where in the EDP system could be defined as the use of electronics such as a computer to process data.

6. **Pramod Damle(2006)**[6], carried out research on a Info-Tech (IT) Security Training imparted in Indian Banks. The study was carried out to assess how IT security training is analyzed, designed and implemented at present in Indian banks and to outline the modification to training need assessment as also the training methodology, where necessary for such courses. The researcher listed the following objective for the study. The researcher concluded that IT security needs significant boost across all levels and functions in banks. The researcher also found that IT security policy is not reviewed and revised periodically.

7. **Najaf Gharachourlou Aghjelou (2007)**[7], in his thesis researcher wrote that risk analysis and risk management have got much importance in the Indian economy during liberalization period. Also the foremost among the challenges

---


faced by the banking sector today is the challenge of understanding and managing the risk. The nature of the banking business is having the threat of risk. For management of risk at corporate level, various risks like credit risk, market risk or operational risk have to be converted into one composite measure. Therefore, the researcher said that it is necessary for measurement of operational risk with other credit and market risk. As per international banking rule (Basel Committee Accords) and RBI guidelines the investigation of risk analysis and risk management in co-operative banks is being most important. The objectives of this research were to verify the integrity of internal risk management systems. During the verification process, the researcher tested independently in proportion to the risk.

It was suggested by the researcher that a properly structured risk identification, analysis, and mitigation process can moderate the risks associated with cooperative banks and it need to develop properly educational programs and workshops. The researcher also found that there is no enough data and useful data system in place for facing with risk management in cooperative bank. Finally, the analysis based on the data collected by the researcher shows that most of the bankers cover only credit risk by using simple methods, it represent need of study to develop other kind of risk analysis methods in cooperative banks.

8. Mrs. Rajani A. Jadhav (2010)\(^8\) carried out research work on the “Problems and Prospects of Bank Computerization – A Study of Selected Co-Operative Banks in Pune”. In the study, the researcher has recommended that the present co-operative banking scenario is far from the anywhere and anytime banking. The main cause of this was unavailability of high level of technological tools and the infrastructural facilities like communication system, networking. The researcher also notes that there was lack of awareness amongst the customers about their rights to various banking facilities; lack of knowledge and skills of

\[8\] Mrs. Rajani A. Jadhav, “Problems And Prospects Of Bank Computerization – A Study of Selected Co-Operative Banks In Pune”, University Of Pune, Pune, 2010
the employees of the banks and also comments that resistance against change in the system by all levels of the employees and management including top executives of the banks.

9. **Mrs. Shubhalaxmi S. Joshi (2010)**[^9] carried out a research work on “A Study Of Information Security Policies In Selected IT Companies In Pune City”. The researcher point out that to ensure success towards reaching to the goals of organization from business continuity point of view, the security of information should be the highest priority for an organization. Researcher also wrote that various studies have come to the conclusion that sensitive corporate information which is of prime importance is vulnerable to security attacks. Today, the key asset is often information.

10. **Mr. Umesh Madhav Inamdar (2010)**[^10], the main objective of this research was to find out ways and means to ensure the existence of UCBs as they are much needed by the society. It aims at the attitude of Board of Directors to face the basic problem with regards to Net Interest Margin (NIM), Asset-Liability Management (ALM) and Risk Management (RM) and to evaluate the present system of fixing prices of various products of the banks and to ensure its capability of maintaining required NIM. It also aims at whether the present system of managing liquidity risk and interest rate risk with its capabilities and inaccuracy in pricing of products, is the main cause of sickness? Further, whether non implementation of ALM and RM is cause of sickness?


[^10]: Mr. Umesh Madhav Inamdar, “Role Of Asset-Liability Management And Risk Management In Pricing Of Products In Urban Co-Operative Banks”, University Of Pune, Pune, 2010.
11. Mahendra P. Kalyankar [11], in his study entitled “A study on positive impact of information Technology in Urban Cooperative Banks”, the researcher studied the application of information technology in cooperative banking – a comparative analysis of scheduled and nonscheduled urban cooperative banks. The researcher also investigated the impact of information technology on business growth, profitability, productivity, deposit mobilization of selected urban cooperative banks. The researcher also studied the customer satisfaction level and operating expenses in selected urban cooperative banks.

12. Devdatta Achyut Divekar(2013)[12] studied "Impact of Core Banking System implementation on Business Performance and Profitability of selected Urban Cooperative Banks in Pune City”. Researcher found that huge investment are made by the banks are justifiable and are in position to yield desire result in terms of improving overall business performance and also they can survive in today CBS environment. Cost of core banking, infrastructure, software, hardware, data center, skilled manpower. Researcher also compare and analysis of business growth in pre and post implementation of CBS.

Culmination: Ph. D Theses submitted to various Universities:

Information technology and the communication networking systems have revolutionized the functioning of banks and other financial institutions all over the world. Customer information is the most important asset for any bank. Therefore to provide security to information is the responsibility of top level management of banks. From the literature review it was found that the study was carried out on various aspects of banking, however no specific study was found focusing on information security aspects in core banking environment of urban cooperative banks which is most important parameter of technology age. Therefore the researcher found,


it is very important to study the information security of core banking system in urban cooperative banks in Pune and Mumbai.

2.3 Research papers and articles published in books, journals and periodicals:
The researcher reviewed the research papers, articles on cooperative banks and internet banking, information technology in urban cooperative banks, information security, information security in banks, information security in cooperative banks in India, information security standard published in research journals, proceedings of national and international level conferences, periodicals and news papers and delineated as below.

2.3.1 Cooperative Banks and Information Technology:
1. B. Muniraja Sekhar Dr. B. Sudhir (2012)[13], In this paper authors write that currently, there are about 1872 urban co-operative banks in India, which form 14% of the banking sector. While the focus has always been on private and public sector banks who are riding the technology wave to emerge as front runners in the global banking arena, cooperative banks, have been laggards when it comes to technology adoption. The drivers of performance for UCBs, as for any organization, includes indicators such as increased employee satisfaction, increased customer satisfaction, financial stability, lower average time to resolution, and innovations in information and communications technology (ICT). Co-operative banks can play a significant role in rural financial inclusion if they ably take advantage of the technology in place. Besides enabling faster services, their decision to bring technology into play will open up possibilities of providing new cost-effective banking products and services to the farming community in particular. It is envisaged that post implementation of CBS including Financial Inclusion, Cooperative banks will also implement internet banking, phone banking, ATM network etc. According to industry watchers, technology deployments like CBS are a big challenge in cooperative banks. Factors such as high costs of implementation and maintenance coupled with lack of regional

language software support for CBS are deterrents. Then, there is the issue of customization. Most solutions available in the market cater to the needs of traditional banks and cooperatives need rather specific levels of customization. Indian customers find it hard to use technologies like ATM and prefer to do transactions over the counter. Manpower constraints exist in this sector. Cooperative banks cannot afford to have IT staff to man IT infrastructure in the way that larger banks can. Finally, there are basic issues like power and rugged terrain that make it difficult to run a CBS or anything else 24x7. At the heart of it, cooperatives are trying to increase the number of transactions in electronic mode. Cooperatives are slowly realizing that their customers are no longer restricted to their community. Also, with a huge youth population, there would be increased demand to adopt modern banking practices. Cooperatives that do not grasp this bit of reality will find themselves driven to extinction.

2. **Dr. Vilas Bhikaji Khandare (2012)**[14], the study was focused mainly on issues in customers' services of urban cooperative banks in Beed district. The study focused on whether urban cooperative banks stands in the atmosphere of liberalization, whether urban banks provide modern services like other banks and whether urban banks can understand the problems of customers. The primary data were collected from 200 customers in the form of questionnaire that were taken 50 from each selected urban cooperative banks in Beed district. The growth performance parameters of urban cooperative banks in Beed district shows on an average positive growth rates during the study period. It is observed from the study that the farmer and female customers of these banks are only 5 and 8.5 percent respectively. 63 percent customers utilize demand draft service; 18 percent customers utilize locker facility, 6 percent customers utilized overdraft facility and 74 percent customer’s utilized clearing and transfer facility. The

Major findings of the study is that 90 percent customers expected electricity bill facilities, 80 percent A.T.M. services and 7.5 percent passport services.

3. **Dr. Yashawant Patil (2006)**[^15] wrote that according to the National Association of Software and Services Companies (ASSCOM), the IT market for banks, $500 million in 2002, is expected to grow by 25 per cent a year for the next few years. An international bank on an average spends around 9% of its revenues on IT annually. In India, state owned banks spend only half a percent of their revenues. Though the private banks spend 4-5 %, they still have a long way to go. In contrast the spending on IT by cooperative banks especially urban cooperative banks in India is comparatively very low than private banks and may end even 0.5 to 2 per cent. It is worth to mention here that nationalized banks in India have taken bold initiatives in deployment of new technology. The cooperative banks are no exception in this technology race and the COSMOS Cooperative Bank, Pune in Maharashtra and the Kerla State Cooperative Bank have moved for core banking solution and many urban cooperative banks are in process of shifting to core banking. The author suggested that the cooperative banks of all levels Viz. state, district and cooperative urban banks therefore have to also ensure that technologies are continuously updated to achieve a high degree of risk management capability. In addition, cooperative banks would need to take measures to have appropriate technology for access control and security concern in today’s highly competitive environment. The cooperative banks thus have to have more attention on Information Technology deployment with IT policies and procedures in place to guide these banks on the lines of prevailing standards and solutions.

[^15]: Dr. Yashawant Patil, “Information Technology Deployment In Cooperative Banks”
http://www.hrd.coop/control/Content/8_10_2006_2_24_20_PMbankingtech.pdf
4. **Jyoti Gupta, Suman Jain (2012)** [16], in their study authors revealed that at present there are several cooperative banks which are performing multipurpose functions of financial, administrative, supervisory and development in nature of expansion and development of cooperative credit system. In brief, the cooperative banks have to act as a friend, philosopher and guide to entire cooperative structure. The study is based on some successful co-op banks in Delhi (India). The descriptive type of research was used in this study in order to identify the lending practices of bank and determining customer’s level of satisfaction. The data collection tools method used were questionnaire and interview of the experienced loan officers.

In this paper the researchers surveyed about 200 customers in Delhi city. The study of the bank’s performance along with the lending practices provided to the customers was herewith undertaken. The study shows that 52% of the respondents say that customer service of the bank is good, 24% says that it is excellent and another 24 % says its average and only 2 % says it’s poor. The study revealed that respondents suggested that the banks should adopt the latest technology of the banking like ATMs, internet / online banking, credit cards etc. so as to bring the banks at par with the private sector banks.

5. **Miss. Banishree Das, Dr Nirod Kumar Palai, Dr Kumar Das (2006)** [17], in their article the authors focused on the problems and prospects of cooperative movements. The authors wrote that 1990s boosted economic growth but high level of poverty and unemployment persist in India. Despite impressive economic growth, the powerful wave of consumerism, computerization and corruption coexists in social life of India. It puts over emphasis on high-tech efficiency of


industrial sector and modern urban service sector at the cost of rural sector. Any development route which bypasses the rural people of India is unlikely to be sustainable. Salvation of the developing economy as vast and diverse as India’s lies only in the transformation and revitalization of its rural economy, which requires people’s empowerment and participation. Neither private sector nor public sector shall promote social welfare. India requires meaningful reforms in the cooperative sector, before complete opening up its economy to the competitive regime, which should ensure: a) higher standard of living for the village people. b) Production for mass consumption. In comparison to the step motherly treatment of the past, cooperatives should be considered an important plank of development. The cooperatives have inherent advantages in tackling the problems of poverty alleviation, food security and employment generation. The cooperatives have huge potential to deliver services in areas where both the state and the private sector have failed.

6. **Mr. Anupam Mitra**(2011) [18] discussed the need of corporate governance in urban cooperative banks in India. The researcher observed that in the post-liberalization period the urban co-operative banks, particularly those in larger towns, are facing tougher competition from commercial banks. Even public sector banks have shrugged off their traditional lethargy and have become very aggressive. One of the vital problems, which vitiate cooperative movement, is the interference of the politicians in the organization. To exercise proper control on their operation in order to safeguard depositors and other stakeholder’s interest, good corporate governance is a mind set, a question of value system, a way of keeping one above one’s personal interest assigning priority to the cooperative interest and the way in which those with power, use that power. It is the reflection of quality of management. The author also suggested that the following factors

need to be taken into consideration while applying corporate governance to the urban co-operative banks:

- Lack of proper and adequate understanding of banking principles at the level of Board of Directors and senior management.
- Lack of professionalization at the board and senior management levels.
- Problems arising because of dual control by RBI and State Co-operative Act.
- Lack of proper accountability at the level of board and political influence.
- Undue importance of the interests of the borrowers at the cost of depositors

7. **Nagarkar U. H., Shivagaje A. J(2014)**[19], in their paper author focused on the information technology deployment in urban cooperative bank. Due to liberalization like many other sectors, banking sector has also undergone a drastic change. Use of information technology and revision of licensing policy has widened geographic scope of banking services (Patil Y.S., 2003). The article was an attempt to take overview of these changes as experienced by bank employees. The study was based on survey of 400 employees from 16 cooperative banks out of 21 banks having their head office in Ahmednagar district. The average proportion of bank employee in sample was 15% of total bank employees. Authors stated that even employees do not have formal computer education with short term training programs on computer. In their paper authors suggested that to update the computer skill banks should periodically arrange the training programs for employees. This will not only update the computer skill but also elevate the confidence of employees. As IT policy of RBI and financial policies of RBI may changes as and when necessary but employees may not be completely aware about it, and hence training programs should also cover these aspects along with IT Act 2008. All functions performed in the banks are not equally important, document

typing and editing is the most important and transaction entry and uploading of
data is least important, importance of other functions is in between. Among the IT
functions creating worksheet, browsing internet, e-mail and SMS, up loading are
very often performed whereas printing reports is least performed. In day to day
operation digital support is most common whereas expert support is rare. In this
paper the experience of bank employee’s revealed that software was fully secured
and hence there are rare chances of forensic transactions. This article revealed that
it is easy for communication and use of software in banking is due to many
reasons such as effort saving, time saving and competitive strength of the banks
were professionalism, customer satisfaction, accuracy, decision making capability
and profit revealed that

8. Vandana Gautam and Dr. B.S. Bhatia (2011) [20], in their paper attempt has
been made by authors to assess the impact of global financial crisis on Indian
rural credit market which is led by cooperative banks. Any major impact on fund
management, productivity, asset quality and business growth of cooperative banks
of Punjab has been analyzed. The study concluded that cooperative banks have
fortunately been able to weather the financial crisis relatively well so far and have
not required state support. This is due to the fact that they have no exposure to
toxic assets, a predominant focus on domestic banking, straight forward banking
products, strong capitalization, and principally conservative risk management. In
spite of cooperative banks being resilient to the crisis some lessons need to be
taken from the present scenario to sustain its position in the competitive era.

[20] Vandana Gautam, Dr. B.S. Bhatia, Cooperative Banks and Global Financial
Crisis, Indian Streams Research Journal, Vol – I, ISSUE – V, June 2011, ISSN:-2230-
7850
2.3.2 Information technology in banking a global perspective:

1. Ala`Eddin Mohd Khalaf Ahmad, Hasan Ali Al-Zu`bi (2011)\textsuperscript{21}, the purpose of this paper was to explore the adoption of e-banking functionality and investigates the impact of e-banking on the outcomes of customers satisfaction namely, loyalty and positive WOM (Word-of-mouth) within the Jordanian Commercial Banks. A purposive sampling technique was employed to recruit 179 customers representing the desired range of demographic characteristics (e.g. gender, age, and computer use), previous internet experience levels and product-related knowledge. This research showed that adoption of e-banking (accessibility, convenience, security, privacy content, design, speed, fees and charges) had a positive effect on Jordanian commercial bank customers' satisfaction, loyalty, and positive WOM.

2. Dina R., Allard C. R., Sandra S. (2004)\textsuperscript{22} stated that e-banking has changed the traditional patterns of banks operations. These changes in technology, competition and lifestyles all have an impact on how banks operate today. With the introduction of e–banking customers are saving money and time. Every bank realizes that they must provide some kind of e–banking to their customers in order to survive. Through e–banking banks can better maintain the relationship with customers, e-banking also increases the revenues of banks and can easily gain competitive advantage through differentiation of banking services.


3. Dr. Mohd Ashraf Ali, Azam Mmalik, Ashraf Imam (2012) [23], in this paper authors discussed the benefits and challenges in the Indian banking sector through E-commerce. Authors stated that the e-banking in India have its own advantages to both the banks and the customers. As India is second largest populous country and the ¾ population lives in rural areas and there is a proper need to divert the efforts the entire areas cities as well as villages. The use of information technology not only reduces the costs of operation but also would be effective, easy to maintain, speedier and highly competitive. The most important requirement for the successful working of internet banking is the adoption of the best security method. The banks cannot remain unapproachable from this perception of e-banking, and they should bring appropriate changes to meet the necessities and challenges of e-banking. The challenges posed by the internet banking are need for standardization of hardware, operating systems, system software, and application software to facilitate interconnectivity of systems across branches and need for high levels of security. The authors also addressed the issue of human relations in a computerized environment.

4. Dr. V. V. R. Raman, Dr. Veena Tewari (2011) [24] wrote in their paper that the number of people touched by and affected by IT technology is enormous and is growing rapidly, especially with the increased availability of the internet. This makes a target audience difficult to define and difficult to reach. The ethical issues themselves are also difficult to define, increasingly complex and diverse, and are growing as rapidly as the technology. Attitudes, perceptions and behavior among users of this technology leave much to be desired. It was also discussed that the importance of IS ethics cannot be overstated in the age of the internet. It is


probably not possible to develop comprehensive ethical guidelines to cover every possible situation of IT misuse. It is also possible to develop ethical guidelines on an ongoing basis to keep pace with changes in the issues. This increases the need for organizations to adhere to a strong set of values to steer them through the minefield of ethical choices with which they are faced as they make business decisions. It is also necessary to ensure that the behavior of the organization is in practice aligned with these values and that employee’s buy into them, so that the organization actually practices what it preaches. This puts extra strain on the "know your customer" policy upon which regulators are so insistent.

5. Mr. V. A. James, Dr. Rupa Gunaseelan (2012) [25], The authors paper analyzed the working results of a large, old private sector banks which had branches all over India and who had successfully implemented CBS, for finding out the changes in their total business development by growth in deposits and advances, effectiveness in nonperforming assets (NPA) management, changes in interest and noninterest income (other income), share values and earnings per share (EPS). This paper analyzed the working results for 10 years (5 years pre and 5 years post CBS period) so that the changes in each parameter can be effectively studied and the rate of change can be well established, thereby giving clear indications to other peer group banks, which are yet to take a decision on CBS implementation.

6. Ms. H. Vasanthakumari, Dr. S. Sheela Rani(2010) [26] wrote in their article “Role Of E – Banking Services in the Banking Sector”, SRM Management Digest – 2010 that banking has changed the traditional patterns of bank’s operations. These changes in technology, competition and lifestyles all have an impact on how banks operate today. With the introduction of e–banking customers are saving money and time since they don’t have to physically visit the bank office.


Every bank realizes that they must provide some kind of e–banking to their customers in order to survive. Through e–banking the banks can better maintain the relationship with customers because with e – banking customers tend to interact more with provided services. It also increases the revenue of banks and can easily gain competitive advantage through differentiation of banking services and thereby an image improvement.

7. **Neha Dixit, Dr. Saroj K. Datta (2010)**[^27] wrote that the numbers of internet users have increased dramatically, but most of them are reluctant to provide sensitive personal information to websites because they do not trust e-commerce security. They list out the factors which are affecting the acceptance of e-banking services among adult customers and also indicated level of concern regarding security and privacy issues in Indian context. The finding depicts many factors like security and privacy, trust, innovativeness, familiarity; awareness level increases the acceptance of e-banking services among Indian customers. The finding showed that in spite of their security and privacy concern, adult customers are willing to adopt online banking if banks provide necessary guidance. They recommended to the banks that they have to increase the level of trust between banks’ website and customers. The importance of security and privacy for the acceptance of internet banking has been noted in many banks study and found that people have weak understanding of internet banking, although they are aware about risk. It was clear those adult customers are ready to adopt online banking if banks take necessary action. Authors suggested following strategies should be applied by banks.

- Banks should ensure that online banking is safe and secure for financial transaction like as traditional banking.
- Educate the customer regarding uses of online banking as well as security and privacy of their accounts.

Banks must emphasize the convenience that online banking can provide to elder people, such as avoiding long queue, in order to motivate them to use it.

- Banks must emphasize the cost saving that online can provide to the elder people, such as reduce transaction cost by use of online banking.

8. P.K. Gupta, Jamia Millia Islamia (2008) [28] studied that internet banking had attracted the attention of banks, securities trading firms, brokerage houses, insurance companies, regulators and lawmakers in developing nations since the late 1990s. The researchers showed that impact of internet banking on cost savings, revenue growth and increased customer satisfaction on industry was tremendous and can be a potential tool for building a sound strategy. However, it has raised many public policy issues before the banking regulators and government agencies. The important suggestion made by the authors was that reliable and systematic information on the scope of internet banking in Indian context was still not sufficient. The paper fills significant gaps in knowledge about the consumer’s perspective of internet banking. The paper identified the weaknesses of conventional banking and explores the consumer awareness, use patterns, satisfaction and preferences for internet banking vis-à-vis conventional form of banking and also highlights the factors that may affect the bank’s strategy to adopt internet banking. It was also addressed that the regulatory and supervisory concerns of internet banking. It was concluded that internet banking in India is only at its primitive stage dominated by the Indian private and foreign banks. The risks associated with internet banking are many, which the banks have to model using sophisticated systems and extensive use of technology. The legal framework as its exits requires an updating to streamline and handle the issues associated with internet banking. The functional model can be used to prioritize perceptual variable concerning consumer behavior so that value to the consumer can be maximized. The banks can focus on strategic consumer groups to maximize its revenues from internet banking. The experiences of the global

economies suggested that banks cannot avoid the internet banking phenomenon, but to gain a competitive advantage, they must structure their business models to suit to Indian conditions.

9. **R.K. Mittal, Sanjay Dhingra**[^29] focused on role of e– banking services in the banking sector in their paper. The authors wrote that banks have invested heavily in the technology such as e-commerce, m-commerce, ATMs, debit cards, data warehousing and data mining, customer relationship management solution software, knowledge management systems etc. In information technology deployment, the new private and foreign sector banks have taken lead over the public and old private sector banks. These banks from day one of their operation, computerized all the transactions. Left with no choice public sector banks have also followed the suite and are in different stages of deployment of technology solutions. In this paper, authors have identified the information technology trends, issues and challenges in banking sector. Some of issues and challenges identified as deployment of open standards technology, balancing the channels of transactions, justification of IT investment in terms of ROI, keeping personal touch with the customers, use of technology by the customers, security concerns, technology obsolescence, penetration of IT in rural areas, outsourcing of IT operations and retaining IT employees. Banks are required to address these issues and challenges effectively to stay in business and growth.

10. **Sharman Lichtenstein, Kirsty Williamson**[^30] from an interpretive study of Australian banking consumer experiences with the adoption of internet banking was discussed in this paper. This paper provided an understanding of how and why specific factors affected the consumer decision whether or not to bank on the


internet, in the Australian context. The findings suggested that convenience is the main motivator for consumers to bank on the internet. The findings also highlight increasing risk acceptance by consumers in regard to internet-based services and the growing importance of offering deep levels of consumer support for such services. Finally, the paper suggested that banks will be better able to manage consumer experiences with moving to internet banking if they understand that such experiences involve a process of adjustment and learning over time, and not merely the adoption of a new technology.

11. Timira Shukla, Anita Singh (2011)[31], In this research paper the authors studied how Information technology (IT) is currently being deployed by the Public Sector Banks primarily the state Bank of India. The role of IT with respect to the maturity of information management systems was also discussed as banks are redefining their focus from the product to a comprehensive single view of the customers. This research paper also highlights how a judicious blend of IT, business processes and data integration solutions are essential to survive and consolidate in the new economy. The basic assumption that IT investments lead to cost reduction and efficiency has been explored. The main aim was to build a collaborative information sharing platform to create repositories that link customer’s data with business processes. The suggestion maid by the researchers was that the focus is not only on the number of ATMs or customers using internet banking but also on the quality of data available as it forms the backbone of any information system to meet emerging business opportunities and challenges.

2.3.3 Online banking information security: Global Scenario
1. Ankur Gupta (2006)[32] described that consumer internet banking, with its ability to reach each and every nook and cranny of the world holds great importance for a

nation like India, where conventional banking services are out of reach for a large proportion of the masses. But to make it a success it requires more than just an adequate internet enabling infrastructure. The author suggested that there is a dire need for an adequate legal and regulatory framework to be put into place. One of the crucial elements of such a legal and regulatory framework will be data protection provisions. The emphasis of this article was on the aspect of data protection in the electronic banking sector.

2. **Atul Bamrara, Gajendra Singh, Mamta Bhatt (2013)** [33], The study was an attempt to reveal the varied cyber attack strategies adopted by cyber criminals to target the selected banks in India where spoofing, brute force attack, buffer overflow and cross side scripting are found positively correlated with public and private sector banks. The potential threat to secure enormous volume of data with a varied community of cyber criminals is a challenge in the current digital era. The major finding of the study are listed as below:

- 60% bank executives agreed that online identity theft has been identified by their bank.
- Attacks through malicious code and Denial of Service attack have been taken place agreed by 54% of the executives.
- Denial of service attacks are increasing with a rapid pace.
- The cases of hacking as well as credit card or ATM frauds have also been identified or reported in the banks.
- Phishing, vishing, spoofing, hacking and online identity theft were some of the major challenges for banks to safeguard their customers and the banks itself.

---

3. Christos K. Dimitriadis (2007) [34], the study presented a security analysis of an internet banking authentication mechanism conducted for a major bank, describing how the attack tree may be deployed. The provision of electronic services, such as corporate and personal funds transfer and retail account management, by banking organizations evolved and spread with the introduction of enhanced communication technologies. However, this novel business opportunity for the provision of banking products and services increases the need for security, especially due to the sensitive nature of the information exchanged. Furthermore, attacks against internet banking authentication mechanisms evolve, decreasing the user’s trust and, as a consequence, the spread of internet banking applications in the market. The specific nature of internet banking systems creates the requirement for specialized knowledge on security issues to be able to effectively conduct an auditing or security evaluation process. More specifically, the information systems (IS) auditor should have the necessary technical and operational skills and knowledge to carry out the review of the technology employed and risks associated with internet banking. Following that requirement, this article studied possible attacks according to which state-of-the-art authentication mechanisms are evaluated. An attack tree is created to propose a guide that an auditor, a security consultant or a security officer may use for conducting a security analysis.

4. Deepshikha Jamwal, Devanand Padha (2009) [35], according to authors when people use the internet, they expect confidentiality and data integrity. Internet banking which is a security-based system, there are various risks issues and internet fraud that can affect the customer’s view of the service quality provided


by the banks. The wireless internet is a recent trend followed by the banking systems in India. This research showed that a large urban population use internet. This paper discussed how to protect customer’s privacy and protect against fraud at providing a specific focus to identify the security issues in Indian banking system. Authors proposed a multifactor authentication technique that is a digital signer device with biometric authentication that not only provides a tamper proof storage for the digital signature but also provides its own display and keyboard. This system improves the security of smart cards by avoiding its dependence on the computer to interface with the user, making it immune to virus attacks and also aging factor of human being. The author mentioned the security issues that help to maintain a high level of public confidence in an open network environment which include: Security, Authentication, Trust, non-repudiation, Privacy, Availability.

5. Diwakar H., Naik A.(2008)[36], in tier paper “Investigation of Information Security Management Practices in Indian Public Sector Banks” author stated that the initiation of financial deregulation, globalization and hence the arrival of new techno-savvy market players with customer centric business model, posed a great challenge to the public sector banks (PSB) in India, who were in banking business for more than a century. These banks quickly realized the need for technology based banking solutions as the only way to be in business and hence onward have started introducing technology based solutions at a faster pace, without reforming their information security management at similar pace, thus exposing themselves to information system related security threats. In this paper, using case study research design and methods an investigative study was conducted on the preparedness and the currently prevalent IT security management practices of PSBs were discussed. The potential vulnerabilities that exist in the system with

specific reference to data leaks, suggestions to safeguard these banks from such threats were presented.

6. Hao Chen, Jean-Pierre Corriveau (2009)[37], stated that there is a continuously growing number of customers who use online banking because of its convenience. This paper considered two current online banking problems. First, a lack of attention and research focusing on security issues relevant to the clients’ side of online banking systems. Second, there are many security products used in online banking systems. However, security testing is still in its infancy and little is available to verify if those security products are working properly. Further authors investigated the current categories, criteria, and approaches for security testing. Further then they sketched out how to design a compliance testing system for the security of online banking. This paper does not attempt to develop a specific testing tool for online banking. The researcher further proposed an approach for security testing based on the international security standards and policies, which may help developers and testers to acquire a good understanding of security testing and develop a general compliance testing system focusing on client side security. The researchers believed that the testing system help customers to increase their confidence when performing transactions through online banking and ensure that the online banking systems meet the relevant security requirements and police in order to lower the risks of being attacked by hacker. The compliance testing approach proposed is still a very sketchy conceptual framework.

7. **Hiltgen A. (2006)**[^38], his article classifies common internet banking authentication methods regarding potential threats and their level of security against common credential stealing and channel breaking attacks, respectively. The authors presented two challenges/responses on internet banking authentication solutions; one based on short-time passwords and one certificate-based, and relate them to the taxonomy above. Further the paper outlined how these solutions can be easily extended for non-repudiation (that is, transaction signing), should more sophisticated content manipulation attacks become a real problem. Finally, author summarized his view on future requirements for secure internet banking authentication and concluded by referencing real-live implementations.

8. **Hisamatsu A., Pishva D., Nishantha G.G.D. (2010)**[^39], discussed that digital information has become a social infrastructure and with the expansion of the internet, network infrastructure had become an indispensable part of social life and industrial activity for mankind. In recent years, the demand for online banking has increased and the number of people who rely on online transactions has tremendously increased. Thus, necessity for a reliable security for online transactions is important ever than before. Furthermore, security concerns still exist among the general public when using online applications. Author’s paper explored why online banking is vulnerable to exploits and introduced some of the modern approaches to secure online banking in an easy to follow manner. This paper, by pointing out pros and cons of existing countermeasure technologies, tried to serve as a tutorial to raise public awareness in information security developments and conceived a model for the future technology.


9. Jaideep Murkute, Hemant Nagpure, Harshal Kute, Neha Mohadikar (2013)[40], this paper explained implementation details of online banking authentication system. Security is an important issue for online banking application which can be implemented by various internet technologies and gap between real world and virtual world can be filled up. While implementing online banking system, secure data transfer need can be fulfilled by using https data transfer and database encryption techniques for secure storage of sensitive information. To eliminate threat of phishing and to confirm user identity, QR-code which would be scanned by user mobile device can be used and weakness of traditional password based system can be improved by one time password (OTP) which can be calculated by user transaction information and data unique at user side like IMIE number of the user mobile device. The banks generates the QR-code using user input transfer information and then user need to recognize as to read the code using their mobile phone, after generate the OTP code using transfer information and the hashed user’s mobile device number in their mobile phone. Finally, terminate the transfer by user typing of generated OTP code on the screen.

10. Maria Nilsson, Anne Adams (2005)[41], in their research paper author discussed growing threats to online banking security (e.g. phishing, personal identify fraud) and the personal nature of the data make the balance between security, trust and usability are very important. However, there was little published research about what influences users' perceptions of online banking security and trust. This study identified that the type of authentication system used can affect users' subsequent perceived control, situational awareness and trust. The results from a


questionnaire and in-depth interviews with 86 participants were triangulated to compare two different authentication processes, namely, a 'security box' (i.e. random system generated passwords at the users' location) and 'fixed passwords' (i.e. user owned and constant). The security box and login procedures were perceived significantly more trustworthy and secure at any location than 'fixed passwords'. Four main concepts were identified: "trust" "the authentication system", "location" and "control".

11. Muhammad Saifuddin Khan, Suborna Barua (2009)[42], Information has been the greatest assets in this competitive age for any business. Especially for banks, to remain competitive and accelerate growth, adoption of new, up to date IT infrastructure is a must. Bangladesh, has witnessed a rapid expansion in the adoption of IT infrastructure with innovative tech-oriented financial products and services and thus rapid growth in the banking industry with increased competition. Therefore, banking industry in Bangladesh is now considered as one of the fundamental industries. This paper tried to explore the state of information security, challenges in ensuring this, and suggested some policy options. The study found that banking sector in Bangladesh are sufficiently vulnerable for different information security threats as they are already using many IT based platforms in regular business. Although almost every bank has its own ICT risk management guideline formulated by the Bangladesh bank, yet these are not implemented with due care in most cases. The sector perceives itself as vulnerable in terms of information insecurity due to varying nature of problems, and thus seeks for primarily government role to initiate a wide information security movement.

12. MWR Labs (2010)[43], “Banking Sector Security”, MWR Labs is the research and intelligence arm of MWR Info Security which performs all technical


investigations into new and emerging threats. The labs team provides a focal point within MWR Info Security through providing research into key technology areas that interface with all client projects. To undertake these projects, MWR labs utilizes the talents of some of the World’s leading information security researchers, who adopted a flexible and novel engagement model that enables the provision of practical solutions to the major risks identified across various industries. This review focused on the banking sector and summarized various research projects completed in the past 12 months. Specifically worked closely with global banking organizations to solve the challenges they have faced. Generally these threats can be categorized into 3 areas:

1. Cyber Attack – A slightly clichéd term but one that does a good job of summing up the continued onslaught of targeted malware and custom exploitation techniques. How can you ensure that your assets are protected against all possible types of electronic attack?

2. Data Loss Protection – How can an organization protect against the loss or theft of sensitive information whether it is organization information or that of their customers?

3. Identity and Access Management – How to validate the identity of individuals accessing systems when they are customers, suppliers and employees?

13. N. P. Singh (2007)\textsuperscript{[44]}, in his research work author analyzed the trends of major activities of the phishing across globe specifically in the banking sector. In addition, author analyzed the reasons for increase in fishing activities, types of phishing techniques, and process of phishing. Further author has presented recent cases of phishing specifically in banking/financial sector. Towards the end the author has studied the measures to fight against the fishing in online banking. The major findings of the study are:

- There is a sharp rise in phishing statistics.
- The main reason for losses/success of frauds is ignorance on part of customer as well as service providers (bankers, and retailers etc).

\textsuperscript{[44]} N. P. Singh, “Online Frauds in Banks with Phishing” Journal of Internet Banking and Commerce, August 2007, vol. 12, no.2
It requires stringent methods of educating customers.

Regular review of security related information of individual customers is required.

14. **Usman Munir, Irfan Manarvi (2010)** [45] stated that advancements in IT have exposed organization to information security threats also. Several methods and standards for assessment of information security in an organization are available today. The problems with these methods and standards are that they neither provide quantitative analysis of information security nor access potential loses information malfunctioning could create. This paper highlights the necessity of information security tool which could provide quantitative risk assessment along with the classification of risk management controls like management, operational and technical controls in an organization. Author suggested that it is not possible for organizations to establish information security effectively without knowing the loopholes in their controls. It was observed that mostly banks have implemented the technical and operational controls properly but the information security culture in organization is still a missing link in information security management.

15. **Yi-Jen Yang (1994)** [46], discussed in his paper that the internet has played a key role in changing how we interact with other people and how we do business today. As a result of the internet, electronic commerce has emerged, allowing businesses to more effectively interact with their customers and other corporations inside and outside their industries. One industry that is using this new communication channel to reach its customers is the banking industry. The electronic banking system addresses several emerging trends: customers demand for anytime, anywhere.
anywhere service, product time-to-market imperatives and increasingly complex back-office integration challenges. The challenges that oppose electronic banking are the concerns of security and privacy of information. The current focus of security of information transfer is on the session layer protocols and the flaws in end-to-end computing. A secure end-to-end transaction requires a secure protocol to communicate over untrusted channels and a trusted code at both endpoints. The solution addressed the use of secure protocols because trusted channels don’t really exist in most of the environment. The solutions to the security issues require the use of software-based systems or hardware-based systems or a hybrid of the two. These software-based solutions involve the use of encryption algorithms, private and public keys, and digital signatures to form software packets known as secure electronic transaction used by MasterCard and Pretty Good Privacy. Hardware-based solutions such as the Smartcard and the MeChip provide better protection for the confidentiality of personal information. Software-based solutions have the advantage over hardware-based solutions in that they are easy to distribute and are generally less expensive.

16. Zakaria Saleh, Izzat Alsmadi (2010) [47], discussed that mobile banking is introducing a new generation of location-independent financial services using mobile terminals. This facilitates allowing users to make payments, check balances, transfer money between accounts and generate statements of recent transactions on their cellular phones. While providing , anywhere, anytime banking to the user, the service should be secure and security needs to be implemented at various levels, starting from the SIM card security, mobile software security, and secure customer access to banking services. Banks rely on users having their mobile phones with them all the time. Hence, as a mean for security measures, banks can send alerts, anytime, in order to provide an enhanced security and services. This paper analyzed the security issues in mobile banking, and proposed an improved security to the mobile banking services using RFID.

2.3.4 Information Security:

1. Abhishek Vaish, Shirshu Varma (2009) [48] writes that information security management and maturity goes side by side. With the growing popularity among the organization to go for the implementation of a structured security management, this also warrants attention of the security community not to escape with the burden of realizing the significance of a mature security management. Additionally, authors also suggested that it is better not to have certified security management system than having immature system. Risk management is the essence of information security management system but the community working in the area of information security had to consider the magnitude of risk the environment will have if the information security management is immature.

2. Angeliki Tsohou, Spyros Kokolakis and Maria Karyda, Evangelos Kiountouzis (2008)[49], The aim of this paper was to identify and analyze approaches adopted by IS security research with regard to information security awareness and to explore whether these ways are consistent with the approaches applied in organization theory and IS Process-variance models 283 for studying organizational processes. The researchers proposed a process-variance typology for the information security awareness research models. The three types of research models (process, variance, and hybrid) identified in the literature analyzed reflect the work performed by security researchers and practitioners. One possibility for future research would be to expand this set of empirical types and develop a new perspective that studies the security awareness in a different basis. The proposed process-variance classification is valuable for a number of


reasons. First, it can help researchers and practitioners understand the distinction between process and variance perspectives, by identifying the key dimensions along which they differ. Second, the categories in the classification identify the range of options available to researchers and practitioners when they design their work.

3. **Asunur Cezar, Huseyin Cavusoglu, Srinivasan Raghunathan (2014)** [50], The researchers examined the implications of a firm outsourcing both (i) security device management which attempts to prevent security breaches and (ii) security monitoring which attempts to detect security breaches to managed security service providers (MSSPs). In the context of security outsourcing, the firm not only faces the traditional moral hazard problem as it cannot observe an MSSP’s prevention or detection effort, but also observes the security breach outcome only imperfectly. Furthermore, outsourced prevention and detection services are separate but interrelated security functions, and thereby cannot be considered independently. Therefore authors suggested that the firm needs to carefully design a contract or contracts to induce the desired efforts from the service providers to effectively manage the cost of information security. The researchers first proved that the current practice of outsourcing both device management and monitoring functions to the same MSSP using a contract that imposes a penalty on MSSP when the MSSP is deemed responsible for a breach results in a higher than the first-best prevention effort and zero (and less than the first-best) detection effort. This is due to the conflict of interest faced by the MSSP and the substitutable nature of prevention and detection services. Authors then proposed two new contracts, both of which achieve the first-best outcomes. The first contract imposed a penalty for a breach and offers a reward for detecting and revealing

breaches to the firm and the second contract calls for the firm to use two different MSSPs - one for prevention and the other for detection. The required penalty and reward are smaller when the firm uses two MSSPs than when it uses a single MSSP. It is possible for all three types of contracts to fail to satisfy the fairness criterion – the penalty does not exceed the firm’s loss from a security breach, and also fail to achieve the first-best efforts when there are limits on penalty and/or reward. However, the two-MSSP contract meets the fairness criterion whenever the other two contracts do. An increase in the prevention cost relative to the detection cost increases the likelihood that the two-MSSP contract meets the fairness criterion, making the two-MSSP contract even more attractive relative to the single MSSP contract with penalty and reward. Despite these advantages of the two-MSSP contract over single MSSP contracts, the firm may be better off outsourcing both prevention and detection functions to the same MSSP with a penalty-and-reward-based contract if a strong cost complementarities exists between the two functions.

4. B. Raja Rao, P. Anil Kumar, K Rama Mohana Rao, M. Nagu (2010) [51], stated that the demand for effective information security schemes is increasing day by day with the exponential growth of internet. Cryptography and Steganography are the two popular techniques for secret communication. The contents of message are kept secret in cryptography, where as in steganography the message is embedded into the cover image (text, video and image (pay load)). In this proposed system authors developed a system in which cryptography and Steganography were used as integrated part along with newly developed enhanced security model. In cryptography MD-5 algorithm was used to encrypt a message and a part of message is hidden in DCT of an image, remaining part of the message was used to generate three secret keys which make the system highly secured. To avoid the problem of unauthorized data access Steganography along

with cryptography called as Cryptic-Steganography scheme was the right most solution suggested by the researchers.

5. **Bryan Cline (2009)** [52] described that the link between security engineering and systems engineering exists at the earliest stage of systems development, and, as a whole, there is sufficient evidence to suggest the discipline of security engineering is sufficiently mature to support its implementation. However, there is little in the literature on the practical application of security engineering and even less empirical work grounded in adoption theory. In contrast, the body of knowledge on quality programs is quite extensive and includes general literature on quality models as well as adoption studies of their implementation. Specific factors related to quality implementations are also well documented and generally well understood. This survey study clearly substantiates a connection between these quality factors and security engineering, provides the opportunity for further research on causal models, and supports the application of lessons learned from quality program efforts to the implementation of a security engineering methodology in system acquisition and development.

6. **Errol A. Blake (2006)** [53] Information Technology (IT) security has been a highlight in every organization since the inception of computer systems. It has been observed that the emergence of various forms of IT security or access controls from passwords to biometrics. This paper discussed the five key points including upper level management’s responsibility to (1) establish and implement a System-Specific Policy (SSP) and Access Control Policy (ACP) for access control, (2) foster an environment of trust with their employees, (3) overlap access control with risk management, (4) establish an optimum level of information

---


security spending, and (5) have a liability or insurance policy for losses. Author suggested that to manage access controls in an organization effectively upper level management should implement an Enterprise Information Security Policy (EISP) or, rather, a System-Specific Policy (SSP) for access control to help management effectively manage access controls. Trust is a very sensitive issue; in the era of the cyber terrorist management are very paranoid of trusting someone with their information whether it is in storage, processing or transmitting. Overlapping access control with risk management by establishing a risk management policy is important. The author suggested that a course of actions must be in place for management in the event something bad may occur.

7. Fariborz Farahmand, Shamkant B. Navathe, Gunter P. Sharp, Philip H. Enslow (2003) [54], in their paper authors discussed that information security-conscious managers of organizations have the responsibility to advise their senior management of the level of risks faced by the information systems. This requires managers to conduct vulnerability assessment as the first step of a risk analysis approach. However, a lack of real world data classification of security threats and develops a three-axis view of the threat space. It develops a scheme for probabilistic evaluation of impact of the security threats and proposes a risk management system consisting of a five-step approach. The goal was to assess the expected damages due to attacks, and managing the risk of attacks.

Further they elaborated on as organizations adopt newer forms of information systems; the complexity of protecting those systems continues to increase. The lack of standards for quantifying the potential cost of computer security incidents was a major problem for the management of information systems revealed by the researchers. Considering these facts, this paper provided assistance for managers

to evaluate the possible damages caused by information security incidents. The researcher reviewed the existing taxonomy of threats to information systems and discussed the potential damages of attacks on information assets and their countermeasures. The classification of assets and a systematic approach to identify costs based on assessed probabilities was also presented. Researchers discussed subjective analysis for the probability assessment of threats to information systems, some possible pitfalls of this method, a possible reasonable approach for using subjective assessment, and a risk management system to manage these threats. Overall, this paper has provided a framework for approaching the difficult problem of security risk vulnerability assessment with which most organizations are confronted today.

8. George Whitson (2003) [55], The internet backbone servers were attacked and web traffic slowed for a few hours, the Nimda worm used Microsoft Web servers to infect all those downloading Web pages until appropriate patches were applied and credit card information is stolen every day. These are just some well known examples of breaches in computer security, but it is difficult to define computer security. This paper presented a high-level overview of computer security that organizes the mass of seemingly unrelated subjects of computer security into a manageable whole. They key concept of the organization is that computer security consists of some basic theory, like cryptography and network protocols; a software engineering process that was used to systematically develop computer security systems and management techniques that are used to keep a computer security system operating. The organization of computer security described in this paper is the result of experiences gained in developing a one semester course on computer security that gives students a real understanding of all aspects of computer security. The course has an introduction to cryptography, but is not overly mathematical. It uses software engineering techniques to develop computer security systems, but does not follow any one known modeling technique. In

this paper researchers described computer security as consisting of three components:


c. Management - Techniques needed to keep the system running.

Viewing the mass of information comprising computer security today, using the above classification provides a reference model that helps both novices and experts organize this material into something manageable. In particular, using computer security engineering to build computer security systems provides an engineering-like method for developing and deploying computer security systems. While this approach to organizing the information of computer security is useful for anyone trying to understand what is going on in the field.

9. **ISACA (2010), “Social Media: Business Benefits and Security, Governance and Assurance Perspectives”[^56]**, This paper discussed the social media’s business benefits and security issues of its. Social media affords enterprises many potential benefits; information risk professionals are concerned about its inherent risks such as data leakage, malware propagation and privacy infringement. The use of social media is becoming a dominant force that has far-ranging implications for enterprises and individuals alike. While this emerging communication technology offers great opportunities to interact with customers and business partners in new and exciting ways, there are significant risks to those who adopt this technology without a clear strategy that addresses both the benefits and the risks. There are also significant risks and potential opportunity costs for those who think that ignoring this revolution in communication is the appropriate way to avoid the risks it presents. The paper suggested that there should be viable approach for each enterprise to engage all relevant stakeholders and to establish a strategy and associated policies that address the pertinent issues.

10. **James William Rust (2005)**[^57] in his paper author discussed that computer forensics is a new and emerging field in information security that requires specialized skills in order to collect and preserve data on systems that have been breached by a hacker, either internal or external to the company. Collecting and processing a digital crime scene can be a difficult, time consuming, and time sensitive task. This paper looked at the various aspects of computer forensics evidence management, from the initial crime and collecting and processing the evidence, through handing the case over to the proper authorities.

In today’s corporate computing environment, it is unrealistic to expect to conduct business without fear of being attacked from any direction. More corporations are employing specialized security teams in an effort to deal with incidents more directly, keep the incident out of the public eye, and to maintain normal business function. In the event that the company falls prey to a hacker or disgruntled employees with an axe to grind the security teams can respond more quickly, contain the incident site, and collect and catalogue pertinent digital forensic data, with greater confidence that the normal workflow and business processes will be restored in a shorter timeframe. It is important to maintain open lines of communication between management and the security team, ensuring that the proper courses of action are taken at every phase of the incident.

11. **Jan Eloff, Mariki Eloff (2003)**[^58] in their paper authors wrote that information security management needs a paradigm shift in order to successfully protect information assets. Organizations must change to the holistic management of information security, requiring a well-established Information Security Management System (ISMS). Organizational management and their staff to manage information security cost-effectively can use the ISMS. An intelligent


mix of aspects such as policies, standards, guidelines, codes-of-practice, technology, human issues, legal and ethical issues constitute ISMS. They suggested that organizations should opt for a combination of these different aspects in establishing ISMS. In order to successfully secure the information and technology related assets of an organization, management should aim towards establishing an ISMS. A well-defined ISMS includes a wide spectrum of issues to be addressed during the planning, management and monitoring of information security within an organization. Apart from the people issues, which are critical to any successful information security program, a relationship between processes as identified in a code-of-practice and certified IT products should be sought after.

12. Liu, Simon, Silverman M. (2001) \[59\], wrote in his paper that as organizations search for more secure authentication methods for user access, e-commerce and other security applications, biometrics is gaining increasing attention. Further authors stated that there is no one best biometric technology. Different applications require different biometrics. To select the right biometric organizations need to navigate through some complex vendor products and keep an eye on future developments in technology and standards. After years of research and development, vendors now have several products to offer. Some are relatively immature, having only recently become commercially available, but even these can substantially improve organization information security posture. The authors briefly described some emerging biometric technologies to guide organizations in decision making.

13. Max M. North, Roy George, Sarah M. North (2007)[60], in today’s global economy, information security and awareness is an absolutely essential component of any management information system. Furthermore, the importance of information security and awareness is even more vital in university environments. Like other organizations, universities provide users with access to an immense amount of information and resources. As such, it is supremely important for students and faculty to be aware of security and ethical issues associated with the usage of these information resources. This paper briefly examined the data collected from a survey of computer science majors and non-majors enrolled in an introductory computer literacy course. The preliminary results of this survey reported that computer science majors were equally or slightly more aware of information security and ethics than non-majors.

The preliminary results of the survey revealed that the need for computer security and ethics awareness for both major and non-major students and suggested that education is one of the most effective ways to improve awareness in this area. One of the most surprising results deals with the fact that more majors than non-majors admitted to violating ethical codes. The authors predicted that one reason for this is that majors are more comfortable with and more aware of computing technology than non-major students. Based on the preliminary results and computations, the following recommendations were offered to increase awareness:

1. Provide special modules to be included in current courses that will give basic information on computer/computing security and ethics.

2. Develop training sessions that will teach students about the installation of antivirus software and firewalls as well as the use of UPS and data backups.

3. Design and post a special section on the university website for students to obtain the latest information and updates on software and related issues.

4. Organize workshops or presentations by technical speakers who are currently working in the industry to provide up-to-date information about computer security and ethics awareness.

14. Max North, DeAnthony Perryman, Shekinah Burns, and Sarah North (2010)[61], This paper revealed that people involved in management information systems face several challenges, especially when it comes to securing their information systems. This is most evident within the university environment, specifically when providing computing resources to students in diverse university environments. There is a common belief that students who attend technology universities have more awareness of security and ethics than those who do not. This study was conducted to compare the levels of information security and ethics awareness of students in diverse university environments. It compares survey data collected from two different university environments—a liberal arts university and technology university. The result of this comparative study showed that students attending the technology university tend to be more aware of security and ethics in information systems than those who attend the liberal arts university. Finally, based on analysis of the collected data, several recommendations were provided to increase the awareness of computer security and ethics in university environments.

There are important and significant differences between understanding of information security and ethical computer use among students in technology universities and liberal universities. The way the individuals are taught and the way the students learn will create a large variance in each culture's perspective. The largest difference in perspective was found in the sections pertaining to firewalls, software updates and patches, uninterruptible power supply, and briefly in the codes of ethics. Members of the technology university had a greater awareness of what a firewall is, as well as its personal and college-based use. The technology students were more aware of software updates and patches to a significant degree. Although neither the technology university nor the liberal university students had an overwhelming awareness of what an uninterruptible power supply is or what it is used for, the technology university was significantly more aware the university campus was using one. In the area of code of ethics, a significant difference presented itself in the questions of using software not paid for or the use of an account for illegal reasons. In reference to the use of software not paid for, the technology college used the software significantly more than liberal student. However, when asked if their account had been used for illegal reasons, the liberal university students said yes significantly more than students of the technology university. Proper measures can be taken to increase awareness among students of both universities including

- Increased exposure to computers.
- Detailed training will ensure proper use and maintenance of the computers.
- Providing the proper tools to the university bodies.
- Offering classes periodically as technology changes.
- Developing an initial university computer awareness class to aid in universal knowledge.
15. Merv Matson, Mihaela Ulieru (2006)[62], this paper introduced a file level information security technology that applies everywhere, every time. The security is always ‘on’, as much ‘in the wild’ as behind the firewall or in the VPN tunnel. The broad strokes of structure and operation are discussed in terms of a specific system, rights enforcer. The technology is currently being deployed in the Adaptive Risk Management Lab at the University of New Brunswick as part of a tested supporting emergency response operations. Persistent information security brings several advantages to the digital world, among which the most significant are:

- Information security now applies everywhere, not just behind the firewall or in the VPN tunnel.
- Access control now applies every time, not just when the user first retrieves the information from the host system.
- The use of information can be tracked, even after distribution to internal and remote users.
- The common digital document delivery mechanisms, email, FTP, shared memory and web download are no longer blocked by insecurity.
- Information custodians can apply peer and policy controls to distributed, circulating documents.

Author experimented with rights enforcer in the Adaptive Risk Management Laboratory in the context of emergency response operations applications, where PIS promises to be very useful, especially:

- For email and document distribution outside the host systems.
- As another very fine layer of security inside the host systems, and for ad hoc and spontaneous confidential communications to and from emergency response personnel and their collaborators and stakeholders.

16. Mikko T. Siponen, Harri Oinas-Kukkonen (2007) [63], this paper identified four security issues 1. access to Information Systems 2. Secure communication 3. Security management and 4. Development of secure Information Systems, and examined the extent to which these security issues have been addressed by existing research efforts. Research contributions in relation to these four security issues were analyzed from three viewpoints: a meta-model for information systems, the research approaches used, and the reference disciplines used. The study revealed that most information security research has focused on the technical context and on issues of access to IS and secure communication. The corresponding security issues have been resolved by using mathematical approaches as a research approach. The reference disciplines most commonly reflected have been mathematics, including philosophical logic. Based on this analysis, authors suggested new directions for studying information security from an information systems viewpoint, with respect to research methodology and research questions. The empirical studies in relation to the issues of security management and the development of secure IS, based on suitable reference theories (e.g., psychology, sociology, semiotics, and philosophy), are particularly necessary.

17. Paul Jeffery Marshall (2010) [64], discussed four scenarios regarding cyber crimes specifically directed at financial institution. The four scenarios discussed regarding online crimes and malicious malware Trojans indicate that financial institutions face major challenges in the coming years defending against high tech robbery and attack by cyber thieves who purpose is to invent ways to ingratiate data systems online to illegally access information, loot, embezzle, and steal money. What if the same minds that create bank malicious malware trojans that


successfully attack financial institution could be rehabilitated and trusted to use that same creative energy to reverse engineer counter attacks against financial cyber crimes. The best offense against cyber crimes is defense against cyber crimes. The author stated that the security of an infrastructure needs to be strong. The enterprise scale virus protection software and engine should be updated and patched real time, and frequent in- formation system security audits to identify risk and vulnerability to a financial institution should be mandatory. Further the author suggested that it is the responsibility of every financial institution’s stakeholder charged with the responsibility as the custodian of electronic information to redouble efforts to do all that can be done to combat cyber crimes. In addition, a secure global centralized database should be created as a watch list to identify cyber-criminals, their crimes, patterns and behavior of malicious and destructive banking Trojans, and any information regarding cyber-pirates and activity. Further author suggested that the goal of financial institution information system security stakeholders to create a secure environment, hacker free safe zone, and make the user experience the best it can be when banking online with a financial institution.

18. Ramgovind S., Eloff M. M., Smith E.(2010) [65], in their research paper author stated that cloud computing has elevated IT to newer limits by offering the market environment data storage and capacity with flexible scalable computing processing power to match elastic demand and supply, whilst reducing capital expenditure. However the opportunity cost of the successful implementation of cloud computing is to effectively manage the security in the cloud applications. Security consciousness and concerns arise as soon as one begins to run applications beyond the designated firewall and move closer towards the public domain. The purpose of the paper was to provide an overall security perspective of cloud computing with the aim to highlight the security concerns that should be properly addressed and managed to realize the full potential of cloud computing.

Gartner's list on cloud security issues, as well the findings from the International Data Corporation enterprise panel survey based on cloud threats were discussed in this paper.

19. Robert M Polstra (2005)[66], this paper showed the importance that management plays in the protection of information and in the planning to handle a security breach when a theft of information happens. Recent thefts of information that have hit major companies have caused concern. These thefts were caused by companies’ inability to determine risks associated with the protection of their data and these companies lack of planning to properly manage a security breach when it occurs. It is becoming necessary, if not mandatory, for organizations to perform ongoing risk analysis to protect their systems. Organizations need to realize that the theft of information is a management issue as well as a technology one, and that these recent security breaches were mainly caused by business decisions by management and not a lack of technology.

As more identity thefts occur, companies that make their money from storing this information are going to become liable. The choice point scandal has been a wakeup call for how vulnerable consumers are to identity theft because of the lack of security standards for the largely unregulated information broker industry,’ said Gail Hillebrand, Senior Attorney for Consumers Union’s West Coast Office.

Author found that companies need to find the importance of protecting their data from both technology and business practices weaknesses. Companies view the protection of their data from a technology issue, but fail to realize the importance that management plays in protecting their systems with the creation of policies and understanding the risks that face their information systems.

From a consumer standpoint, if a company is making profit from someone’s personal information and they fail to protect this data, should they not give some

sort of reputation? Companies own and manage consumer information, and individuals have little power over their information that is controlled by these organizations. As identity theft continues and companies fail at protecting their data, legislation will be passed that will force companies to comply with regulator standards that may force companies to give this reputation to individuals who have their identity stolen.

Further the author suggested that there are steps that companies and organizations need to take to protect themselves from the theft of information. The steps that were suggested by author are listed below:

- Companies need to be prepared when a security breach occurs because a risk to an asset is never zero percent.
- Organizations need to establish policies and risk assessments that protect their data from both technology risks and business practices well before a security breach occurs.
- This is achieved by companies having the organizational structure that allows management to fully understand the business processes and technology that expose their information systems to threats.
- Also, companies need the ability to change and adapt to new threats that oppose their information.
- It is not possible to prevent all security breaches that lead to a theft of information, but companies will need to have policies and practices in place to better protect the data.

Companies will need not only to weigh technology risk to their information, but also understand business issues that expose their information to theft. It no longer matters how the information stolen, whether it was a hacker or a social engineer that committed the crime; companies need to protect their information from all threats and minimize their risks from all aspects.
20. Sh. Ladan, A. Yari, and H. Khodabandeh(2006)\cite{67}, discussed that the need for information security in organizations, regardless of their type and size, is being addressed by emerging standards and recommended best practices. The various standards and practices which evolved in recent years and are still being developed and constantly revised, address the issue of information security from different angles. This paper provided an overview of information security standards and practices. Through a comparative study of their similarities and differences, some insight can be obtained on how their combination may lead to an increased level of information security. This comparative study has shown that each of the examined documents approach the issue of security from different angles. ISO 17799 and BS7799-2 attempt to provide a total solution for information security, reaching a practical level of implementation in the form of controls. COBIT is designed to be the breakthrough IT governance tool that helps in understanding and managing the risks and benefits associated with information and related IT. Authors suggested that in order to achieve better security of information and products it is recommended to combine different security standards. For an Information Security Management System implementation effective, one should be able to objectively measure its compliance to the directives and principles by which it is designed. The issue of security compliance and measuring still remains open and a great amount of research effort is expected to be directed in this area.

21. Thompson H.(2012) \cite{68}, discussed in his paper entitled “The Human Element of Information Security, Security & Privacy” that information security has long hinged on trusted insiders' ability to make good decisions. However, modifying human behavior through training is difficult; some battle-worn security executives


might even dismiss it as impossible. Although foundational controls such as antivirus, data leak protection, and firewalls are important, they're far from sufficient. The sharp rise in "know ability" of people at a distance raises an important question for the information security industry about the automation of personalized attacks. Today, most security controls are ignorant of rich historical data about the person they're tasked with protecting. As the cost for attackers to personalize their attacks goes down, our zeal in building technology to personalize defense must rise. This article explored industry’s need to embrace security's human element.

2.3.5 Various articles published in News papers on information security:

1. Core banking challenges and solutions (2008) [69], Banks have attained more leeway on the technology front than ever before. From just being a business enabler, IT is now a business driver for the banking sector. At the heart of banking technology, lays the Core Banking Solutions (CBS) implemented by most banks. CBS is nothing but automation of banks across multiple delivery channels. The article wrote that CBS helps banks achieve a centralized processing mechanism and in turn provide an 'anytime anywhere' service to their customers. However, core banking applications come with their set of challenges as well.

With intense competition and changing market dynamics, banks have to brace themselves for newer obstacles every now and then. Moreover, fresh regulations and compliance requirements, industry consolidation, delivering cost effective products and services, maintaining secure data platforms, meeting ever increasing customer demands and other strategic issues have all made banking far more complex than it used to be in the past. In order to handle increasing transaction volumes and do away with issues hovering around the current systems, banks need the right CBS in place.

Banks need is a flexible, customer centric core banking environment that is also equipped with multi-currency and multi-lingual features since the industry is getting increasingly globalised. For instance, Canara Bank recently enabled CBS

at as many as 1000 branches, which is one of the largest implementations in the banking industry and includes agricultural loans, loan processing, foreign exchange and service branch functionality. This has helped the bank move in line with the changing market scenario.

At present, out of the total IT spending undertaken by banks, around 75 per cent goes toward maintenance of existing systems and ensuring that the business of the bank goes through smoothly. Hence, a major exercise in upgrading core banking architecture is something many banks may not be able to afford at present. To gain an edge over their competitors and address customer demands effectively, banks need to do a balancing act by replacing old systems with new platforms, without giving up on existing core banking modules which might still cater to changing needs. There has been considerable progress in CBS implementation by banks; however, there is much more ground left to cover.

2. RBI's IT vision document calls for its use beyond CBS (2011) [70], MUMBAI: The Reserve Bank said it will soon be implementing new information technology guidelines which call upon banks to use IT beyond the current core banking solutions and into newer areas like management information systems and regulatory reporting.

The RBI released its 'IT Vision Document for 2011-17' which calls on commercial banks to use IT in areas like MIS, regulatory reporting, overall risk management, financial inclusion and customer relationship management.

The document, prepared by a High Level Committee chaired by Deputy Governor K C Chakrabarty, also dwells on possible operational risks arising out of adopting technology in the banking sector which could affect financial stability.

The IT vision document emphasizes the need for internal controls, risk mitigation systems, fraud detection/prevention and business continuity plans. The vision document noted the use of technology for analytical processing by banks was still at a nascent stage.

"The report urges banks to work towards reaping benefits of technology in terms of cost reduction of small value transactions, improved customer services and effective flow of information within the banks and to the regulator. The vision document stresses on transforming the RBI into an information intensive knowledge organization and adopting appropriate business process re-engineering.

3. Net banking fraud most common cybercrime (2013) [71]: Higher internet connectivity in Millennium city has also given cyber crimes a bigger playing field.

Of the total 759 cases of online crime recorded in the past year by the police, 248 were related to bank fraud, making it the most common among cybercrime cases registered by the police.

   - In 2012-2013, phishers launched attacks affecting an average of 1,02,100 people worldwide each day – twice as many as in 2011-2012.
   - Phishing attacks most often target users in Russia, the USA, India, Vietnam and the UK.
   - Vietnam, the USA, India and Germany have the greatest number of attacked users – the total number of attacks in these regions has doubled since last year.
   - Over 20% of all phishing attacks mimicked banks and other financial organizations.

5. 8,322 Cyber Frauds Cases Registered In Banks In 2012 (2013) [73]: The Reserve Bank of India has registered 8,322 cases of cyber frauds in 2012, a

decline from 9,588 cases and 15,018 cases registered in 2011 and 2010 respectively. This announcement was made by Namo Narian Meena, the Minister of State for Finance, in a written reply to the Lok Sabha. RBI informed that these cyber frauds include frauds recorded in ATMs, Debit Cards, Internet Banking and Credit Cards. It also mentioned that this includes data for 48 banks and the organization has not included data for banks that have turned into non-performing assets. The minister stated that around Rs 52.66 crore were involved in these cyber fraud cases in 2012, a significant increase from Rs 36.72 crore in 2011 and Rs 40.48 crore in 2010.

6. **RBI asks urban Co-operative Banks to implement CBS by Dec 3, 2013**

The article stated that Reserve Bank India asked urban co-operative banks (UCBs) to implement core banking solutions (CBS) in all their branches by December 31, 2013."...very few UCBs have adopted CBS. Hence all UCBs are advised to implement CBS, in all their branches before December 31, 2013,"

It further stated that the failure to implement CBS within the time frame could result in denial of various facilities like expansion of branches or area of operation to UCBs. The usage of Information Technology (IT) is critical for the survival and growth of banking institutions as IT usage not only helps banks to reduce their cost of operations, but also enables them to offer products and services at competitive rates to their customers.

Also, IT is not just an enabler but a differentiator for banks in a competitive environment. Further, for effective regulatory and supervisory compliance the banks need to use IT in their operations. It also mentioned that CBS helps to integrate range of services that can be offered by all the bank's branches from centralized data centers. The Government of India has also observed that UCBs without CBS do not integrate well with the banking system and hence there is the need to quickly adopt this model. CBS is a necessity in today's banking scenario.

and therefore, advised in their own interest, as also in the interest of their customers, to adopt CBS as soon as possible.

7. **RBI warns banks against cyber attacks (2013)** [75]: This article stated that the Reserve Bank of India directed banks to periodically check their preparedness to prevent any cyber attack. Considering that cyber attacks could threaten the confidentiality, integrity and availability of data and the systems, it is imperative for banks to conduct VAPT (vulnerability assessment and penetration testing) periodically to prevent any such attacks. In the communication to heads of banks, it is stated that there is a need to ensure that gaps identified from the tests are plugged in a timely manner. This should form part of the information security assurance function undertaken by banks”. RBI has been emphasizing to banks on the importance of putting appropriate IT and information system (IS) governance structures to enable better control and security.

It further stated that formulation of consolidated business continuity plans (BCPs) documents by banks covering critical aspects of people, process and technology is important in view of the increased contribution of 24x7 electronic banking channels.

8. **Cyber attacks on the rise in India (2014)** [76]: The ease of online banking and transactions has brought with it a significant rise in malicious attacks on digital devices and software systems. Most of these attacks, as recent instances of online thefts have demonstrated, have been in the banking and financial services domain. According to reports by research agencies, the problem has become more complex with the proliferation of mobile devices and the users' preference towards transactions on the go. In addition, there is also laxity on the part of the users when it comes to following safe practices during such transactions, coupled with a significant lack of manpower with skills to handle the rising number of such attacks, the agencies' reports state.

[75] http://businesstoday.intoday.in/ New Delhi , June 27, 2013
The article stated that India has seen significant increase in attacks against financials and government, with 34% and 43% of them reporting cyber threats and attacks respectively, up from last year's 15% and 19%, the report revealed. Matthew Moynahan, president of Arbor Networks, said that From the ISP to the enterprise, IT and security teams are facing a dynamic threat landscape and very skilled and patient adversaries. He further added that multi-layered defenses are clearly needed, but so is a commitment to best practices for people and process. The article also stated that another report from EC-Council foundation pointed at a major gap in information security threat handling capabilities in India. The report showed talent levels in nine crucial segments of information security, the implications of which could impact handling of cyber threats in industries such as banking and economy, defense, healthcare, information and energy among others.

9. Two held for ATM card fraud (2014) [77], Jamshedpur, District police have busted a racket involved in fraudulent withdrawal of cash from ATM kiosks and arrested two youths in this connection. Accused Rakesh Yadav and Sanjeev Sikdar used to secure account details from customers posing as bank officials before withdrawing money with duplicate debit cards. The duo made phone calls to anonymous bank customers and collected account details from them. They used to threaten the customers of suspending the account if details are not furnished immediately. After collecting the account details the duo passed on the information to their aides who eventually withdrew cash using clone ATM cards.

10. Woman gives caller ATM pin, loses Rs 62,000 (2014) [78], NAGPUR: Using a new trick, an unidentified caller took the ATM pin code from a 35-year-old woman and withdrew cash Rs 62,000 from her account. The victim Seema Rangari, a resident of Chandramani Nagar, works with the social welfare department. She told police that she received a call from a private bank on March 31. The caller first asked for her ATM code, saying that it was required for some bank purpose. He later told her to add some digits to it.

11. “Six men uproot ATM machine holding Rs 8 lakh & take it away” (2014)[79],

A group of six men stole an ATM machine of the State Bank of India (SBI) in North-east Delhi’s Bhajanpura area in the wee hours of Sunday after plucking out the CCTV camera installed in the ATM booth to leave no proof behind. The CCTV footage from the ATM booth was lost as the hard disk containing the footage was stolen along with the machine. No guard was present at the spot when the theft took place. The thieves worked from 2:35 am to 3:05 am to uproot the machine. The men slice off the base of the machine using a gas cutter. After plucking out the wires from the machine, they dragged the machine out and loaded it into the tempo and left.

Conclusion:

This chapter has enclosed a wide range of knowledge about literature review related to the information security. The reviewed literature on information security highlights problem on information security in online banking implementation including organizational and social issues. The researcher had broadly studied literature from several perspectives of information security. In this perspective, literature review was done to discover the gaps that existed between appropriate existing material and proposed study. Exploring the literature concerned with the effectiveness evaluation of information security controls in core banking environment concluded the lack of available studies in this particular area of research. One reason for this is that this area of research is comparatively new. Furthermore, the majority of the studies in this domain are conducted on a micro level and related with studies from the fields of business management, computer science, and sometimes engineering and they were generally in the form of reports or descriptive studies, and rarely practical ones.

The existing research in information security related to online banking implementation showed that there is still lack of studies in the present literature about the information security in CORE banking environment in urban cooperative banks. The researcher also found that there is still an increasing need for comprehensive but

[79] https://in.news.yahoo.com/, Mail Today, 7th April 2014
specific approaches to information security aspects that would assist management in implementation of effective information security program not only in CORE banking environment of urban cooperative banks but providing the technology based solution including internet banking.

The researcher found that most of research studies carried out across the globe on internet/online banking, information security were mainly focuses on the following area:

- Information security policies in selected IT companies
- Info-Tech (IT) security training imparted in Indian banks
- Banking On IT: Problems and Prospects in State Bank Of India
- Ethics and IT- Unsolved issues of online based banking
- E-Commerce : Benefits and Challenges in Indian banking sector
- Acceptance of E-banking among adult customers
- Comfort Your Online Customer: Quality, Trust, and Loyalty on the Internet
- Internet Banking In India – Consumer concerns and bank strategies
- Internet Banking Systems in India: Analysis of security issues
- Understanding Consumer Adoption of Internet Banking: An interpretive study in the Australian banking context
- Business Benefits and Security, Governance and Assurance Perspectives
- The ‘How’ and ‘Why’ of Persistent Information Security
- “Information Security Management – A New Paradigm
- The Management of Access Controls/ Biometrics in organizations
- Organizational barriers to the implementation of security engineering
- Proposed next generation information security management effectiveness measurement model
- Analyzing the security of internet banking authentication mechanisms
- Information Security risk assessment for banking sector-a case study of Pakistani banks
- The Status and Threats of information security in the banking sector of Bangladesh: policies required
- The Security of Electronic Banking
- Data Protection in Consumer E-banking
Online Banking: Information Security vs. Hackers
Information Technology in Banking Sector: Trends, Issues and Challenges
Role Of E – Banking Services in the Banking Sector
E-banking functionality and outcomes of customer satisfaction: an empirical investigation
Internet Banking in India – Consumer, Concerns and Bank Strategies
Internet Banking Systems in India: Analysis of security issues
Computer Security: Theory, Process and Management
A review of information security issues and respective research contributions
Security management of mutually trusted domains through cooperation of defensive technologies
Managing vulnerabilities of information systems to security incidents
Study of information security and ethics awareness as an imperative component of management information systems
Combination of information security standards to cover national requirements
Security testing and compliance for online banking in real-world
Outsourcing Information Security: contracting issues and security implications
The security of electronic banking implementation of core banking solution (CBS) and subsequent business development, in old private sector bank

The researcher also found that most of the research studies carried out on urban cooperatives bank was mainly focuses on the following area:

Management of funds of selected urban co-operative bank in Maharashtra
Cooperative movement in Maharashtra
Role of urban co-operative bank in Maharashtra state
Co-operative study of personnel policies and practices in commercial banks and co-operative banks
Problems and prospects of bank computerization - selected co-operative banks in Pune
Risk analysis and risk management in selected branches of cooperative banks in Pune
Role of asset-liability management and risk management in pricing of products in urban co-operative banks
Information Technology Deployment in Cooperative Banks
Core banking solutions in urban cooperative banks- Issues and Challenges
Corporate governance of urban co-operative banks in India: An overview
Impact of information technology in urban cooperative banks
Impact of core banking system implementation on business performance and profitability of selected urban cooperative banks in Pune City

This literature review has made it possible to identify many of the possible issues in the area of information security. Researcher conducted an extensive review of the literature to identify the key attributes of information security and related issues and the gaps identified from the literature review are listed below:

- Sensitive corporate information which is of prime importance is vulnerable to security attacks.
- Security of information should be the highest priority for an organization.
- There is no enough data and useful data system available to deal with risk management in urban cooperative bank.
- Focus is not only on the number of ATMs or customers using internet banking but also on the quality of data available as it forms the backbone of any information system to meet emerging business opportunities and challenges.
- Cooperative banks would need to take measures to have appropriate technology for access control and security concern in today’s highly competitive environment.
- The cooperative banks have to have more attention on information technology deployment with IT policies and procedures in place to guide these banks on the lines of prevailing standards and solutions.
- Reliable and systematic information on the scope of internet banking in Indian context is still not sufficient.
- People issues, which are most critical issue to any successful information security program.
- Security testing is still in its infancy and little is available to verify if those security products are working properly.
- There is a need for an adequate legal and regulatory framework to be put into place.
- The security of an infrastructure needs to be strong.
The enterprise scale virus protection software and engine should be updated and patched real time, and frequent information system security audits to identify risk and vulnerability to a financial institution should be mandatory.

The lack of prevailing standards for quantifying the potential cost of computer security incidents is a major problem for the management of information systems.

Information security and awareness is an essential component for effective information security management.

The issue of security compliance and measuring still remains open and a great amount of research effort is expected to be directed in this area.

Development of secure Information Systems.

Lack of awareness amongst end user about the information security.

Need for well-established Information Security Management System(ISMS).

There was hardly any study which focused on information security in urban cooperative bank. It was found from the literature review that there was not a single study carried out on information security system for CBS environment in urban cooperative banks of Pune and Mumbai.