Chapter – 8
SUMMARY OF
FINDINGS,
SUGGESTIONS AND
CONCLUSIONS
Chapter – 8

SUMMARY OF FINDINGS, CONCLUSIONS AND SUGGESTIONS

8.1 Summary of Findings:

The following are the findings of research study:

I. **Effect of security standards on online Banking:**
   
   Due to adoption of security standards has resulted in preventing data loss and easy fraud detection. Especially all the banks in India were made to adopt various security standards such as PCI-DSS, ISO 27001/27002 to give users a highly secured and robust online banking environment.

II. **RBI regulatory enablers to encourage online Banking:**
   
   Guidelines are in place as latent countermeasures to achieve fraud detection such as zero liability for cardholders and nationwide insurance for protecting the customer from frauds. Zero liability for customer for cyber fraud loss has made banks more vigilant in monitoring and on site action. Currently US banks offer $50 for any cyber fraud loss by the customer. In India some banks offer 2000.

III. **Current e-fraud preventive measures for online Banking:**
   
   Real time soft computing techniques such as AI heuristics, pattern recognition, fuzzy logic, neural networks, data mining etc., can be effectively used in cyber fraud prevention.

   Technology facilitators for efficient and secured online transactions. For example adoption of EMV chip technology, Biometric technology, E-Lock digital signature etc., Security has to be a global solution, as banking is now one global inter-connected system.

IV. **Current security measures in practice:**
   
   The following are the security measures followed by most of the banks in India and abroad. These measures have been implemented in the following devices and point of transactions.

   a. Point of access – privacy of transactions.

   b. Communication exchange listening.

   c. Processing storage and software applications.
d. Majority of security standards implemented are adopted standards, mostly from US and practiced globally which is based their banking environment. We need to develop domestic standards that are suitable and applicable to local environment. Along with the existing security measures and taking into consideration Indian environment, new security measures have been adopted by banks and periodic RBI guidelines has a positive impact on online banking services, which has resulted in marginal reduction in cyber fraud in India.

V. The impact of Online Banking:

1. Exposure to world market. Online Banking has changed the face of transactional business and affects commerce in many trades and industries across the globe.

2. Ability to compete with international banks in terms of: better customer services, check clearance, Electronic Fund Transfer (EFT), electronic payment, any-time-anywhere customer web access with safe and secured life style.

3. Advantages in commercial banking. Online Banking can be performed on 24x7 basis. Consumers with Internet access can log in to their banks website any time of the day and perform any number of banking transactions. Unlimited access provides consumers with the convenience of doing business on weekends and holidays when banks are traditionally closed.

4. Reduction in paper usage. The online is more economical, secure and has high accessibility to the required Information at any time. This has resulted in reduction in use of paper in banks substantially which also help in conservation of nature. The mandatory adoption of PCI- DSS in 2006 has increased user’s confidence. This has paved the way for more and more online banking services in India, which has direct impact on reduction in paper usage.
8.2. Suggestions:

1. Majority of banks have no in-house grievances remedial system. This is a necessity in Indian banks which reduces online frauds drastically. This grievance redressal system permits the affected customers to come forward to report fraud immediately so that tracing of frauds will be easy for banks as it is done in real time and is in closed loop system.

2. While adopting the security measures enacted in the US and the European countries, Indian banks should be able to confer to international security measures and adopt the latest technology based on the effectiveness of the internationally tested security system.

3. Online customers should be made aware of the security measures taken by banks and educated periodically with notifications for carrying out safe and secure transactions.

4. The training of bank employees should be carefully designed with specific emphasis on ‘security standard and cyber laws’. It should be a dynamic program as security standard and cyber laws change from time to time.

5. A good security policy is a must for fraud-free transactions. This should be evaluated for every three months based upon the feedback from all the stakeholders.

6. RBI guidelines have to be followed strictly and implemented immediately to counter any fraud.

7. Banks should follow and implement global security standards periodically to minimise the fraud.

8. There is a gap in understanding the information technology between technical and non-technical people in the banks. This should be narrowed with proper training in information technology especially with its implemented security measures and security policy of the banks.

9. To have safe and secure ATM/Online transactions follow BBB or 3B’s (Basic, Biometrics , Behavior metrics) security model which provides the customer with substantial reduced risk and fraud in online transactions.
10. Banks should adopt automatic customer warning and alert system either through mobile SMS or E-mail or ringtone or voice mails for any type of online financial transactions.

8.3 Conclusions:

After analysing the adoption of security standard PCI-DSS in Indian banks using both primary and secondary data the following conclusions are drawn.

1. The banks in India have adopted the e-security vis-à-vis on par with foreign banks while understanding the technology by bank personnel is a matter of concern.

2. The foreign banks have robust security as they have given top priority for privacy of customers data as they experienced large data breach in e-banking for several years.

3. The bank personnel in Indian banks are trained to understand the security but are unable to solve immediate e-security breach because of the inadequate technology perception.

4. Though there is a high secured technology, there are weak links in terms of total adoption of technology due to lack of proper understanding of the security methods by its stakeholders.

5. The PCI-DSS is ever emerging credit/debit card standard. Also it has minimised cyber fraud to greater extent due to its continuous periodic evaluation from time to time.

6. The Indian banks irrespective of their type of banking the security measures taken by them are good and their security policy is in tune with periodically issued RBI guidelines. The RBI guidelines has played a major role in reducing cyber frauds.

7. Impact of IT ACT 2000/2008 on cyber fraud is not upto the expectations of law makers due to slow implementation.

8. The security in Indian banks are comparable to foreign banks.

9. Indian banks require more in-house technical personnel to handle any reported cyber fraud.

10. The PCI-DSS adoption in Indian banks are satisfactory.
8.4. Scope For Future Work:

PCI-DSS 12 requirements has given a fairly good security for card holders data. Still there is a gap in the adoption and implementation of PCI-DSS in banks. The researcher feels that individual requirement analysis of all 12 requirements and its relations to technology, security policy of each organisation should be studied. The study on the adoption of PCI-DSS and fraud analysis in countries having highest broadband connectivity may throw light on new challenges in core security issues of global cardholder. To have highest security in online transactions the research study may be done on adoption of behaviour trait of user as one of the security metrics.