SECURITY AND PRIVACY ISSUES IN E-BANKING: AN EMPIRICAL STUDY OF CUSTOMERS' PERCEPTION

A

MACRO RESEARCH PROJECT

REPORT

(2012-13)

SUBMITTED TO

INDIAN INSTITUTE OF BANKING AND FINANCE (IIBF)

MUMBAI

DR. TEJINDERPAL SINGH
ASSISTANT PROFESSOR
UNIVERSITY BUSINESS SCHOOL
PANJAB UNIVERSITY CHANDIGARH

OCTOBER 2013

DECLARATION

I hereby declare that this project report entitled, "Security and Privacy Issues in E-Banking: An Empirical Study of Customers' Perception" is a bonafide and genuine research work carried out by me under the Macro Research Award 2012-2013 of Indian Institute of Banking and Finance (IIBF) Mumbai

Date: 4/10/2013 Signature

Place: Chandigarh **(Dr. Tejinderpal Singh)**

ACKNOWLEDGEMENT

Research is like an endless ocean and one needs to be guided and supported by several individuals in order to derive out a handful of pearls from its depth. I take this opportunity to express my deep sense of gratitude to all those who made this research possible.

I wish to express my sincere gratitude and regards towards Indian Institute of Banking and Finance Mumbai, for awarding me Macro Research Award 2012-2013 to provide me an opportunity to conduct this research study.

I duly acknowledge the services of AC Joshi Library, Panjab University, Chandigarh and Department Libraries of University Business School and Department of Economics, Panjab University Chandigarh

I express my sincere thanks to the officials of selected banks who have supported me in the form of providing valuable information to accomplish the project.

I will be failing in my duties if I don't express my sincere gratitude to all bank customers who responded the queries contained in the questionnaire and interview schedule.

I lack words to express my gratitude to my loving wife Dr. Harmeet Kaur, who had contributed with his practical help and support throughout the course of study. Her lucid way of scientific expression is one thing that I would definitely try to follow always. Last but not least, I am thankful to my parents, brother, my in-laws family and my loving daughter Palak who were right behind me throughout the difficult phases of this research pursuit. It was for their forbearance, help and inspiration that this work could be completed on time. All of my friends, relatives and well wishers whose names I am unable to count also deserve my thanks for their moral support to me.

Last but not least, my heartfelt salutations to the lotus feet of the Almighty God for always being there, whenever my faith faltered.

Date: *(Dr. Tejinderpal Singh)*

Place:

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

3G	Third Generation
AIMC	Amount of Information about Mobile Phone Credit Card
ATM	Automated Teller Machine
ATT	Attitude
CERT	Computer Emergency Response Team
CNP	Card Not Present
CR	Customer Readiness
CSIBAM	Customer Specific internet banking acceptance model
CV	Customer Value
CVV	Card Verification Value
DMA	Direct Marketing Agent
DSA	Direct Selling Agent
DTH	Direct To Home
ECS	Electronic Clearing Service
EMV	Europay, MasterCard and Visa
EVSSL	Extended Validation Secure Socket Layer
FIR	First Information Report
GPRS	General Packet Radio Service
IB	Internet Banking
IBS	Internet Banking service
IDS	Intruder Detection System
IP	Internet Protocol
IT	Information Technology
KMAC	Key Based Message Authentication
KYC	Know Your Customer
MFA	Multi-factor Authentication
MITB	Man In The Browser
MITM	Man In the Middle Attack
MOTO	Mail Order Transaction Order
MPRI	Mobile Payment readiness Index
NBFC	Non Banking Financial Company
NEFT	National Electronic Fund Transfer

NRI	Non-Resident Items
OPT	One time Password
PA-DSS	Payment Application - Data Security Standard
PBC	Perceived Behavioral Control
PC	Personal Computer
PCI-DSS	Payment card Industry – Data Security Standard
PE	Perceived Expressiveness
PEOU	Perceived Ease of use
PIN	Personal Identification Number
PLS	Partial Least Square
PNB	Punjab National bank
POS	Point Of Sale
PPL	Perceived Playfulness
PR	Perceived Risk
PU	Perceived Usefulness
RBI	Reserve Bank of India
RTGS	Real Time Gross Settlement
SBI	State Bank of India
SEM	Structural Equation Modeling
SSL	Secure Socket Layer
SST	Self Service Technologies
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TAM	Technology Acceptance Model
TPB	Theory of Planned Behaviour
TRA	Theory of Reasoned Action
UK	United Kingdom
URL	Uniform Resource Locator
URN	Uniform Resource Name
USB	Universal Serial Bus
UTAUT	Unified Theory of Acceptance and Use of Technology
VOIP	Voice Over- Internet Protocol
WAP	Wireless Application Protocol
WLA	White Label ATMs

ABSTRACT

Problem Statement: "Security and Privacy Issues in E- Banking: An Empirical Study of Customers' Perception"

Objectives: The purpose of the study is to compare the security and privacy features of selected banks online banking portals. Study further examines the bank customers' perception towards 'security & privacy concern' and security & privacy satisfaction' regarding use of e-banking services. Lastly, it studies the opinion of non-users of e-banking services.

Research Methodology: Four banks were selected for study purpose. Security and privacy features of online banking portals were compared with the help of check list. To study the customers' perception a survey was conducted by administering the questionnaire to 200(190 Final) bank customers in the tri-city i.e. Chandigarh, Mohali and Panchkula. One-way ANOVA, Kruskal Wallis test and Person's coefficient of correlation was used to test the hypotheses.

Results: Study found that selected banks differed on security and privacy features of online banking portals. Few banks have advance security features in their online banking portals and others still have traditional security features. The level of security and privacy concern is moderate regarding use of ATMs whereas it was found high in case of Internet Banking, Mobile banking and Credit Cards. The level of satisfaction regarding security and privacy with respects use of all selected e-banking services was high. Further there was negative correlation between bank customers' perception towards 'security and privacy concern' and security and privacy satisfaction. Non users of e-banking services cited security and privacy concern as one of reasons for Not Using E-Banking Services.

Research Implications: The findings of the study have implications for banking industry in two ways. Firstly, the comparison of security and privacy features will help the bankers to make their online portal more secure by incorporating the security features which other banks are using. Secondly, the study will be helpful to the bankers to understand the behavior of internet banking users and behaviour of non-internet banking users.

Originality: In the present study eight new construct have developed to measure the security &privacy concern and security & privacy satisfaction regard use of various e-banking services. Further, this is first study of this kind conducted in India where customers' perception rereading security and privacy has been studied in detail.

Key words: *Concern, e-banking, Online banking portals, Privacy, Security and Satisfaction.*

Chapter – 1
INTRODUCTION

1.1 BACKGROUND OF THE STUDY

As the new millennium and information age progress, organizations around the world are going through massive transformation efforts to cope with the constantly changing business market trends .Volatile financial markets have all added to the pressure on organizations to come up with effective responses to survive and succeed. Furthermore, easing of international trade barriers, economic liberalization, globalization, and deregulation have led to several challenges for organizations in developing and newly industrializing economies (Laisuzzaman et al., 2010) like India. To effectively respond to the rapid changes in the external environment, several firms have turned to information technology to improve their productivity and competitiveness. Until the mid-1990s, many Indian organizations had operated under a protected economic regime, limited competition, and a regulated environment. This had resulted in limited focus on process efficiencies, centralized control structures, highly formalized business settings, and lack of professional business practices. However, following the economic liberalization and opening up of the economy to foreign competition, Indian organizations have been forced to adopt modern business practices and strategies. In an effort to enhance their competitiveness, several organizations have turned to information and communication technology to improve business processes and exploit efficiencies in the value chain (Kannabiran, 2005).

The development of communication and information technologies has encouraged the emergence of new distribution channels that have enhanced the options available to businesses for building relationships with clients: for

communication activities, customer distribution, customer satisfaction control, post-sale service etc. Nowadays, simultaneous use of various channels is increasingly more important, which gives rise to the need for a multichannel contact strategy for clients. Albesa (2007) asserts that businesses should seek a multichannel configuration that provides 'channel advantages', because each channel presents some differential strengths, but at the same time presents limitations and complications, in this way, the use of a single channel limits performance in the market to what that channel is capable of doing particularly well. Likewise, desires and different expectations from clients can require different information and contact strategies

Convergence of technologies has made the distribution of services more convenient than ever before. Automatic Teller Machines, bill payment kiosks, internet based services and phone based services (both voice and text), automated hotel check out, automated check-in for flights, automated food ordering system in restaurants, vending machines, Interactive voice response systems are examples of technology based service delivery channels. Amongst various service industries, banks sector has been mostly influenced by the information technology.

1.1.1 Information Technology and Indian Banking Sector

The Indian banking system has come a long way since independence from nationalization to liberalization. It has witnessed transition from a slow business institution to a highly proactive and dynamic entity. This transformation has been largely brought about by liberalization and economic reforms that allowed banks to explore new business opportunities rather than generating revenues from conventional streams of borrowing and lending. These financial reforms that were initiated in the early 1970s brought in a completely new operating environment to the banks. The banks are now offering innovative and attractive technology based multi channels to

offer their products and services. The process started in the 1970s when computers were introduced as 'ledger posting machines'. Technology has been deployed in variety of back-office and customer-interface activities of banking. In the early 1980s Reserve Bank of India set up two committees to accelerate the pace of automation of operations in banking sector. A high-level committee was formed under the chairmanship of Dr. C. Rangarajan, to draw up a phased plan for computerization and mechanization in the banking industry. The focus was on customer service. For this purpose, two models of branch automation were developed and implemented. The second Rangarajan committee constituted in 1988 drew up a plan for computerization and automation to other areas such as funds transfer, e-mail, BANKNET, SWIFT, ATMs, i-banking etc.

In the last decade, information technology has brought significant changes in the banking sector. It has provided an opportunity to banks for offering differentiated products and services to their customers using technology platforms. Apart from operations, advancement in technology has played an important role in the distribution strategy of commercial banks (Baraghani, 2007). Banks, which were traditionally relying on sole channel i.e. 'branch' to deliver services have now started offering their product and service through variety of innovative and technology based channels which include channels such as 'Internet Banking', 'Automated Teller Machines (ATMs)', 'Mobile Banking', 'Phone Banking', 'TV Banking' etc. All these new channels of distribution are within the domain of e-banking or i-banking. Electronic banking has been around for quite some time in the form of automated teller machines (ATMs) and telephone transactions. In more recent times, it has been transformed by the internet – a new delivery channel that has facilitated banking transactions for both customers and banks (Nitsure, 2003). As a part of strategic

decisions, banks in India have been investing and continued to invest enormous amount of funds on computer and related technologies expecting substantial payoff (Surulivel and Charumathi 2013). According to The Boston Consulting Group (2011), the current expenditure on information technology (IT) for banks on the whole is Rs 6,500 Cr. per year, about 2.7 per cent of their revenues is further likely to shoot up to Rs 10,000 Cr. annually in the coming years (Malvika Joshi, Sep 2011). Further, Reserve Bank has laid special emphasis on technology infusion in the day to day operations of banks. The IT Vision Document, 2011-17 of the Reserve Bank sets out the roadmap for implementation of key IT applications in banking with special emphasis on seamless delivery of banking services through effective implementation of Business Continuity Management (BCM), Information Security Policy, and Business Process Re-engineering (RBI, 2012).

1.1.2 Present Scenario of E-Banking in India

The evolution of e-banking has fundamentally transformed the way banks traditionally conduct their businesses and the ways consumers perform their banking activities (Eriksson et al., 2008; Sayar and Wolfe, 2007). Today e-banking has experienced phenomenal growth and has become one of the main avenues for banks to deliver their products and services (Amato- McCoy, 2005). Electronic banking (e-banking) is defined as the automated delivery of new and traditional banking products and services directly to customers through electronic, interactive communication channels (Daniel, 1999; Sathye, 1999). E-banking includes the systems that enable financial institution customers, individuals or businesses, to access accounts, transact business, or obtain information on financial products and services through a public or private network, including the internet. Customers access e-banking services using an intelligent electronic device, such as a personal computer (PC), personal digital

assistant (PDA), automated teller machine (ATM), kiosk, or Touch Tone telephone. Chou and Chou (2000) identified five basic services associated with online banking: view account balances and transaction histories; paying bills; transferring funds between accounts; requesting credit card advances; and ordering checks for more faster services that can be provide by domestic and foreign bank.

E-banking offers benefits for both banks and its customers. From the banks' perspective, e-banking has enabled banks to lower operational costs through the reduction of physical facilities and staffing resources required, reduced waiting times in branches resulting in potential increase in sales performance and a larger global reach (Sarel and Mamorstein, 2003). From the customers' perspective, e-banking allows customers to perform a wide range of banking transactions electronically via the bank's website anytime and anywhere (Grabner-Kraeuter and Faullant, 2008). In addition, customers no longer are confined to the opening hours of banks, travel and waiting times are no longer necessary, and access of information regarding banking services are now easily available (Hamlet, 2000). Following delivery channels/ services primarily constitute the domain of e-banking:

1. Automated Teller Machines (ATMs)
2. Internet Banking
3. Phone Banking
4. Mobile Banking
5. TV Banking
6. Non-Cash Retail Payments: Debit Cards, Credit Cards, ECS, NEFT, RTGS

The brief description of these channels has been covered in the subsequent sections.

Automated Teller Machines (ATMs)

Automated Teller Machine is a computerized machine that provides the customers of banks the facility of accessing their account for dispensing cash and to

carry out other financial & non-financial transactions without the need to actually visit their bank branch on insertion of an encoded plastic card (www.msn.encarta.com). ATMs generally accept ATM debit cards, credit cards and prepaid cards (that permit cash withdrawal) for various transactions. Majority of ATM users use ATM to withdraw the cash, however, in addition to cash dispensing ATMs may have many services/facilities enabled by the bank owning the ATM such as; Account information, Cash Deposit, Regular bills payment, Purchase of Re-load Vouchers for Mobiles, Mini Statement, Loan account enquiry etc. For transacting at an ATM, the customer inserts /swipes his card in the ATM and enters his Personal Identification Number (PIN) issued by his bank. Once PIN is accepted by ATM a customer can perform the transaction selected by him. PIN is the numeric password which is separately mailed / handed over to the customer by the bank while issuing the card. Most banks require the customers to change the PIN on the first use.

The present position of ATMs in India has been shown in Table 1.1

Table 1.1
Position of ATMs of Scheduled Commercial Banks
(As on end March, 2012)

Bank group	On-site ATMs		Off-site ATMs		Total number of ATMs		Off-site ATMs as per cent of total ATMs	
	2010-11	2011-12	2010-11	2011-12	2010-11	2011-12	2010-11	2011-12
Public sector banks	**29,795**	**34,012**	**19,692**	**24,181**	**49,487**	**58,193**	**39.8**	**25.27**
Nationalised banks	15,691	18,277	9,145	12,773	24,836	31,050	36.8	13.35
SBI Group	14,104	15,735	10,547	11,408	24,651	27,143	42.8	11.92
Private sector banks	**10,648**	**13,249**	**13,003**	**22,830**	**23,651**	**36,079**	**55.0**	**23.86**
Old private sector banks	2,641	3,342	1,485	2,429	4,126	5,771	36.0	2.54
New private sector banks	8,007	9,907	11,518	20,401	19,525	30,308	59.0	21.32
Foreign banks	**286**	**284**	**1,081**	**1130**	**1,367**	**1414**	**79.1**	**1.18**
All SCBs	**40,729**	**47,545**	**33,776**	**48,141**	**74,505**	**95,686**	**45.3**	**50.31**

Source: RBI, Report on Trend and Progress of banking in India, 2012

Table 1.1 shows that during 2011-12, an additional 21,000 ATMs were deployed by the scheduled commercial banks. Public sector banks accounted for more than 60 per cent of the total number of ATMs as on end of March 2012, while close to one-third of the total ATMs were attributable to new private sector banks. Table further shows that percentage of **'**Off-site ATMs to total ATMs' has been increased from 45.3 percent to 50.31 per cent**.**

Recently, RBI has observed that banks have played a major role in encouraging ATM adoption and modifying behavioral strategies in the domain of personal banking. The banking space has seen considerable growth through the ATMs, (approximately 95000 ATMs at present) but the same has been restricted principally to the urban or metro areas. Tier III to VI unbanked/under banked areas have not witnessed much ATM presence. Although there has been about 30% year-on-year growth in the number of ATMs deployed in the country since 2008, ATM penetration on a per capita basis continues to be less compared to other countries. Therefore, there is an ample scope to deploy more ATMs, particularly in Tier III to VI areas of the country. In the above context, RBI has decided to permit non-banks to set up, own and operate ATMs to accelerate the growth and penetration of ATMs in the country. Such ATMs will be in the nature of White Label ATMs (WLA) and would provide ATM services to customers of all banks. Such entities should have a minimum net worth of Rs. 100 Cr. at the time of making the application and on a continuing basis after issue of the requisite authorization[1].

[1] RBI, DPSS.CO.PD. No. /02.10.002/2011-2012, February, 2012.

Internet Banking

The last decade has witnessed a remarkable growth of internet users in India and all over the world. There are one hundred and thirty seven million internet users in India with 11.4 per cent penetration (Internetworldstats.com). It is predicted that number of internet users in India will reach to at least 300 million users by 2014 up from now (Rajan Anandan) predicted. Such growth is primarily attributed to investment by telecom carriers in high-speed wireless infrastructure and slashing prices of smart phones (online.wsj.com). The promising growth of internet users in India as well as world-wide (566.4 %, 2000-2012) (internetworldstats.com) has presented an optimistic view of future of internet banking in India. Hence, banks are investing huge amount in the infrastructure to host internet banking activities.

Internet Banking also called as online banking is the new age banking system. Internet banking uses the internet as the delivery channel to conduct banking activities like transferring funds, paying bills, viewing account statements, paying mortgages and purchasing financial certificates of deposits, etc. **(**Singhal and Padhmanabhan, 2008). Dinz (1998) developed a model to classify the services delivered through internet banking into three roles having different levels like basic, intermediate and advanced levels of services under each role. The different roles mentioned for internet banking are:

a. Informational: for providing information
b. Transactional : for conducting transactions
c. Relationship: for improving customer relationship

According to RBI's Report of Internet banking (2001) the levels of banking services offered through internet can be categorized into three types:

i. The *basic level service* is the banks' websites which disseminate information on different products and services offered to customers and members of public in general. It may receive and reply to customers' queries through e-mail.

ii. In the next level are *simple transactional websites* which allow customers to submit their instructions, applications for different services, queries on their account balances etc.; but do not permit any fund-based transactions on their accounts.

iii. The third level of internet banking services are offered by *fully transactional websites* which allow the customers to operate on their accounts for transfer of funds, payment of different bills, subscribing to other products of the bank and to transact purchase and sale of securities, etc.

In India, ICICI bank was the first bank to offer online banking way back in 1996 with the launch of 'infinity'. After ICICI Bank, Citibank, IndusInd Bank, HDFC Bank and Times Bank (now part of HDFC Bank), were the early ones to introduce online banking in India (Rajneesh De and Padmanabhan, 2002). At present, majority of commercial banks are offering internet banking service in India (Table1.2)

Table: 1.2
Alexa Ranking of Public and Private Sector online Portals
(As on 20th October, 2012)

Public Sector Banks			
Name of Bank	**Online Portal**	**Alexa Ranking**	**Rank**
State Bank of India	https://www.onlinesbi.com/	61	1
IDBI Bank Ltd.	http://www.idbi.com/	713	2
Punjab National Bank	http://www.netpnb.com/	760	3
State Bank of Hyderabad	https://www.onlinesbh.com/	966	4
Union Bank of India	http://www.unionbankonline.co.in/	1032	5
Bank of India	https://www.bankofindia.com	1042	6
Bank of Baroda	https://www.bobibanking.com/	1,220	7
Oriental Bank of Commerce	https://www.obconline.co.in/	1,361	8
Indian Overseas Bank	https://www.iobnet.co.in/	1369	9
State Bank of Travancore	https://www.sbtonline.in/	1427	10
Indian Bank	https://www.indianbank.net.in/jsp/startIB.jsp	2024	11
Corporation Bank	https://www.corpretail.com/	3359	12
Syndicate Bank	https://netbanking.syndicatebank.in/netbanking/	4047	13
State Bank of Mysore	https://www.onlinesbm.com/	5532	14
State Bank of Patiala	https://www.onlinesbp.com/	6,151	15
State Bank of Bikaner & Jaipur	https://www.sbbjonline.com/	6,886	16
Andhra Bank	https://www.onlineandhrabank.net.in/	7736	17
Dena Bank	http://www.denabank.com/DenaInternetBanking/	8,908	18
Central Bank of India	https://www.centralbank.net.in/	10,632	19
Vijaya Bank	https://www.vijayabankonline.in/	12284	20
Canara Bank	https://www.canarabank.in	13,316	21
UCO Bank	www.ucoebanking.com	13,411	22
United Bank of India	https://unitedbankofindia.com	14272	23
Bank of Maharashtra	https://www.mahaconnect.in/	14,376	24
Allahabad Bank	https://www.allbankonline.in/	15,222	25
Punjab and Sind Bank	https://www.psbindia.com/	38,645	26
New Private Sector Banks			
HDFC Bank Ltd.	http://www.hdfcbank.com/	24	1
ICICI Bank Ltd.	http://www.icicibank.com/	34	2
Axis Bank Ltd.	http://www.axisbank.com	94	3
Kotak Mahindra Ltd.	http://www.kotak.com/	405	4
IndusInd Bank Ltd.	http://www.indusind.com	767	5
Development Credit Bank Ltd.	http://www.dcbbank.com/	32140	6

Source: Compiled from www.Alexa.com[2]

Internet banking is predicted to transform and revolutionalize traditional banking industry (Mols, 2000). Banking services are easily digitalized and automated

[2] Alexa Internet, Inc. is a California-based subsidiary company of Amazon.com which provides commercial web traffic data.

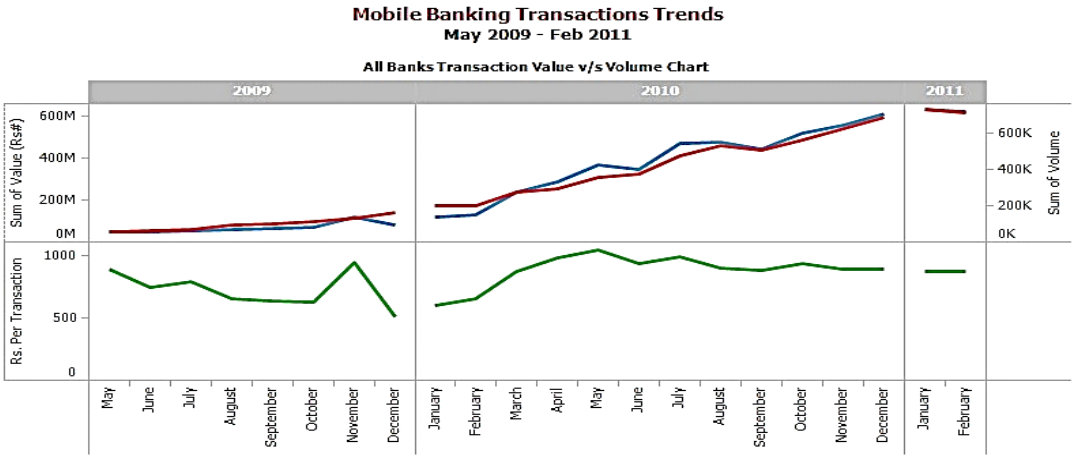
and, thus, from an operational perspective, lend themselves to the internet (Elliot and Loebbecke, 2000; Daniel, 1999) the potential competitive advantage of the internet for banks lays in the areas of cost reduction and satisfaction of consumer needs.

Mobile banking

Mobile banking refers to financial services delivered via mobile networks using mobile phones. RBI defines 'mobile banking' as – "Undertaking banking transactions using mobile phones by bank customers that involve credit/debit to their accounts." It also covers accessing the bank accounts by customers for non-monetary transactions like balance enquiry etc. For customers, mobile banking is convenient while banks benefit through a low-cost channel. Presently, there is no cap on per-day transactions for encrypted transactions in banking channels, including mobile banking. These limits are set by individual banks depending on their risk perception of the respective channels. However, for unencrypted transactions, such as those through SMS, the RBI has set a limit of Rs 5,000 per day.

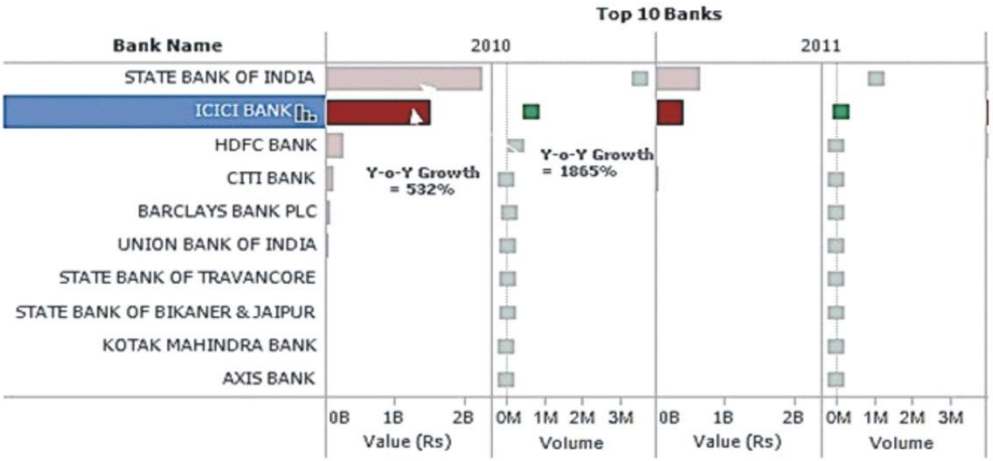
The progress of mobile banking in India during the period May 2009- Feb 2011 and list of top ten banks has been depicted in Figure:1.1 and Figure 1.2 respectively.

Figure 1.1: Progress of Mobile Banking



Source: Source: http://charts.medianama.com/india-mobile-banking-transactions/

Figure 1.2 Top Ten Banks



Source: Source: http://charts.medianama.com/india-mobile-banking-transactions/

Sum of volume,
Sum of value
Amount per transaction

In 2010, SBI posted a Y-o-Y growth of 1865% in transaction values, ICICI posted a growth of 532% and HDFC posted 512% growth.

Table 1.3
Progress of Mobile Banking in India
(From February, 2012 to November 2012)

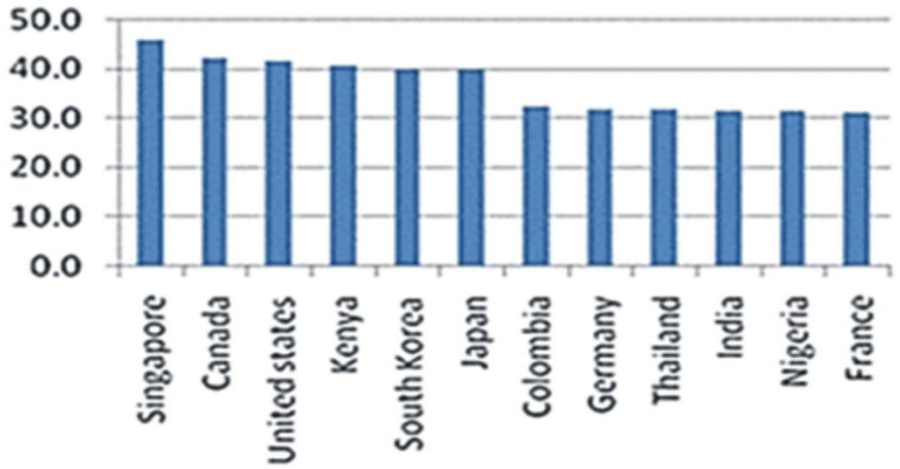
Month (2012)	Volume	Value ('000)	Share in Total Volume			Share in Total value		
			Co-operative and Public Sector	Private and Foreign	State Bank Group	Co-operative and Public Sector	Private and Foreign	State Bank Group
February	2799554	1960417	2.3	12.1	85.6	3.7	46.0	50.3
March	3123105	2325321	2.3	13.7	84.0	3.5	49.0	47.5
April	3178405	2345678	2.4	14.4	83.3	4.0	49.2	46.8
May	3346743	2865454	2.4	18.4	79.2	3.9	56.4	39.7
June	3437074	3067107	2.4	20.6	77.1	3.9	58.3	37.8
July	3705690	3379715	2.4	21.1	76.5	3.9	59.3	36.8
August	3968226	3548628	6.4	22.5	71.1	4.0	60.6	35.4
September	3897614	4104519	3.2	24.3	72.6	4.0	59.0	37.0
October	4437342	7790473	2.7	27.7	69.6	2.5	73.5	23.9
November	4720871	5389548	2.5	30.1	67.4	4.0	61.6	34.5

Source: Compiled from www.rbi.org.in.

Table 1.3 shows that 3.7 Crore mobile transactions took place between February and November 2012, increasing around 1.7 times in volumes over this 10-month period. These transactions saw nearly a three-fold increase in value over the same period. Increasing smart phone adoption and initiatives such as media promotions and customer education programmes for mobile banking have led to this uptrend. Table further shows that SBI group dominates this space in volume terms with an overall share of 67.4 per cent in total volumes followed by Private and foreign banks with an overall share of 30.1 per cent in November 2012. Table also indicates that SBI group (34.5%) has a lower share in value terms compared to the private and foreign banks (61.6%) during the same month. RBI data further reveals that SBI leads with 65.4 per cent share in the total number of mobile transactions carried out in November, followed by ICICI Bank (14.2%), Axis bank (9.4%) and Citi bank (3.5%). Around three per cent of SBI's total customer base is into mobile banking transactions. For ICICI Bank, over 10 million customers have currently registered for mobile banking.

Prepaid mobile recharges, DTH recharges, ticket bookings (movies/travel) are among the fast growing transactions in mobile banking. (Business Standard, January 25, 2013).

Figure 1.3Mobile Payments Readiness Index (MPRI)



Source: http://mobilereadiness.mastercard.com/the-index.

With mobile phone penetration of over 80 per cent, India has a huge potential for mobile banking. But on the global landscape, mobile payments have a long way to go in India. According to the MasterCard Mobile Payments Readiness Index (MPRI), India ranked 21st among 34 countries with the score of 31.4 on a scale of 100. The index is a data-driven survey of the global mobile payments landscape. It relies on an analysis of 34 countries and their readiness to use three types of mobile payments: person to person, mobile e-commerce and mobile payments at the point of sale (POS). The index also points out that consumers in India have not yet fully embraced mobile payments. Only 14 per cent of Indian consumers are familiar with both P2P and m-commerce transactions, and 10 per cent are familiar with POS transactions. Singapore topped the charts with a score of 45.6 followed by Canada and the US with scores of 42 and 41.5, respectively.

Phone banking

Phone banking is a useful channel where customers use an automated phone answering system with phone keypad response. Variety of transactions like account balance information, list of latest transactions, electronic bill payments, funds

transfers etc can be carried out. Phone banking is usually supplemented with call centers where phone banking user has facility to speak to a live representative of the bank at its call centers

TV banking

TV banking has been recently introduced as a joint initiative of ICICI Bank and Dish TV. The service launched in 2009 enables user to access Bank's product information on their Dish TV enabled TV sets. The service is at initial stage with only general information capability and is yet to grow to the level of enabling account specific information, transactions etc.

Non Cash Retail Payments: Debit Cards, Credit Card, ECS, NEFT, RTGS

In India, cash continues to be the pre-dominant mode of payment. The policy initiatives and the regulatory stance of the Reserve Bank has been focusing on increasing the acceptance and penetration of safe, secure and efficient non-cash payment modes comprising cheques, credit/debit cards, and transactions through ECS/RTGS/NEFT, over the years. RTGS system is a funds transfer mechanism where transfer of money takes place from one bank to another on a "real time" and on "gross" basis. This is the fastest possible money transfer system through the banking channel. On the other hand, National Electronic Funds Transfer (NEFT) system is a nationwide funds transfer system to facilitate transfer of funds from any bank branch to any other bank branch. ECS is a mode of electronic funds transfer from one bank account to another bank account using the services of a Clearing House. This is normally for bulk transfers from one account to many accounts or vice-versa. Due to the policy initiatives taken by RBI, the average ratio of non-cash retail payment to GDP continues to hover around 6 per cent over the last three years (Table1.4).

Table 1.4
Trends in Payment Systems (Billion)

Year	Non-cash retail payments*	Non-cash retail payments to GDP ratio	Currency in circulation as a percentage of GDP
2006-07	1,94,459	4.53	11.77
2007-08	3,05,382	6.12	11.85
2008-09	3,29,736	5.91	12.38
2009-10	4,06,116	6.29	12.38
2010-11	4,76,291	6.21	12.36
2011-12	5,16,332	5.83	12.04
*Cheques, ECS, NEFT, Cards, RTGS Customer transactions.			

Source: RBI, Report on Trend and Progress of banking in India, 2012.

Further, Volume and Value of Electronic Transactions by Scheduled Commercial Banks as on end march 2012 has been shown in Table 1.5.

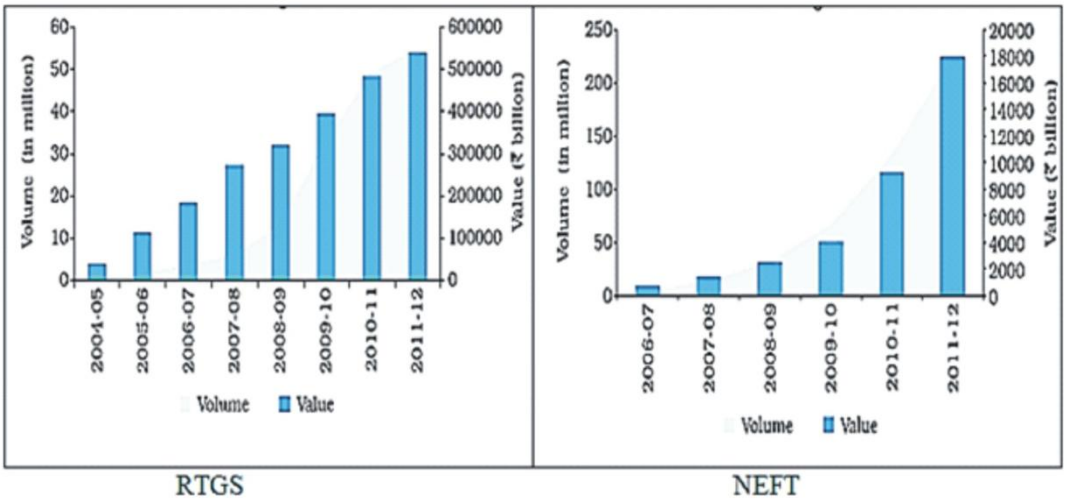
Table 1.5
Volume and Value of Electronic Transactions by Scheduled Commercial Banks (As on end march 2012)

Electronic Transactions	Volume (million)		Percentage Variation		Value (billion)		Percentage Variation	
	2011	2012	2011	2012	2011	2012	2011	2012
ECS Credit	117	122	19.5	3.6	1,817	1,838	54.5	1.2
ECS Debit	157	165	5.0	5.1	736	834	5.9	13.3
Credit cards	265	320	13.2	20.7	755	966	22.2	27.9
Debit cards	237	328	39.3	38.2	387	534	46.6	38.0
NEFT	132	226	99.5	70.9	9,321	17,903	127.6	92.1
RTGS	49	55.0	48.5	11.6	4,84,872	5,39,307	22.9	11.2

Source: Report on Trend and Progress of banking in India, 2012.

Table 1.5 shows that amongst electronic transactions, NEFT has registered the highest growth of 70.9 per cent in number of transaction during the year 2012 followed by Debit Card (38.2%), Credit Card (20.7%), RTGS (11.6%), ECS-Debit (5.1%) and ECS Credit(3.6%) . Similar trend was observed in Value of transaction also.

Figure: 1.4 Progress in RTGS and NEFT Transaction



Source: RBI, Report on Trend and Progress of banking in India, 2012.

Debit card and Credit Cards constitutes an important part of non- cash Transactions. The progress of debit and credit cards issued by Scheduled Commercial Banks has been shown in Table 1.5.

Table 1.5
Credit and Debit Cards Issued by Scheduled Commercial Banks
(As at end-March) (in millions)

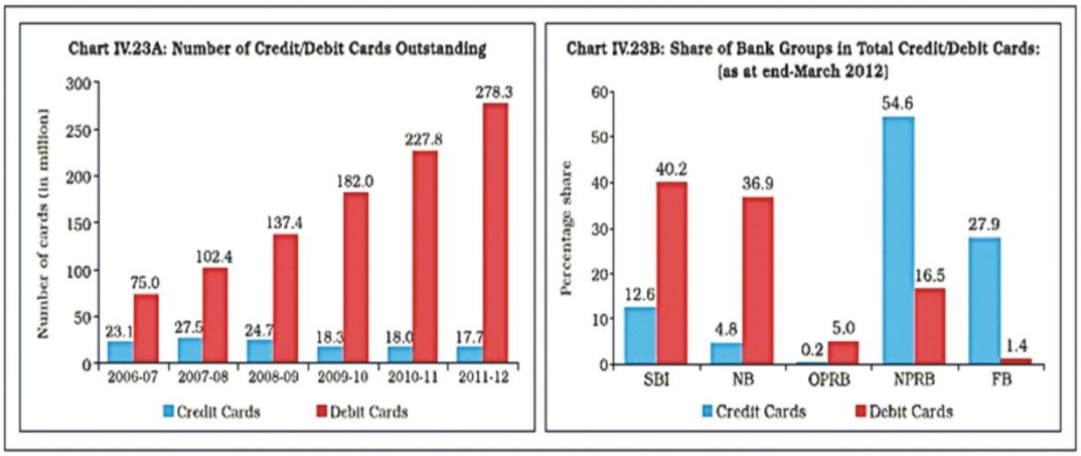
Bank Groups	Outstanding Number of Credit Cards (in millions)		Outstanding Number of Debit Cards (in millions)		Percentage share in total Credit Cards		Percentage share in total Debit Cards	
	2011	2012	2011	2012	2011	2012	2011	2012
Public sector banks	3.08	3.06	170	215	17.07	17.34	74.56	77.34
Nationalised banks	0.78	0.84	80	103	4.32	4.76	35.09	37.05
SBI group	2.30	2.22	90	112	12.75	12.58	39.47	40.29
Private sector banks	9.32	9.67	53	60	51.66	54.79	23.25	21.58
Old private sector banks	0.04	0.04	12	14	0.22	0.23	5.26	5.04
New private sector banks	9.28	9.63	41	46	51.44	54.56	17.98	16.55
Foreign banks	5.64	4.92	3.9	3.8	31.26	27.88	1.71	1.37
All SCBs	18.04	17.65	228	278	100.00	100.00	100.00	100.00

Source: RBI, Report on Trend and Progress of banking in India, 2012.

Table 1.5 shows that issuance of credit cards declined from 18.04 to 17.65 million cards in the year 2012, while debit cards showed a high growth trend by increasing from 228 to 278 millions. Foreign banks, however, showed a small decline in the issuance of debit cards. More than three-fourths of the total debit cards

outstanding as at the end of March 2012 were issued by public sector banks. In contrast, more than half of the outstanding credit cards as at the end of March 2012 were issued by new private sector banks.

Figure 1.5 : Number of Credit/ Debit Card Outstanding and Share of Bank Groups in Total Credit/Debit Cards



Source: RBI, Report on Trend and Progress of banking in India, 2012.

Further, Table 1.6 shows the Progress in credit card number of transactions and amount of transactions for the period of August, 2012- May 2013.

Table: 1.6

Progress in credit card Number of Transactions and Amount of Transactions (August, 2012- May 2013)

Month (2012/13)	No of Credit cards	No. of Transactions (Actual)		Amount of transactions (Rs Million)		Percentage share in total number of credit cards		
		ATM	POS	ATM	POS	Public Sector Banks	Private sector Banks	Foreign Sector Banks
August	18237281	209236	32524725	1217.51	95843.50	17.83	55.59	26.58
September	18379623	198862	30427400	1353.92	93665.38	17.84	55.57	26.59
October	18533052	261213	35583728	1282.25	108643.43	17.84	55.72	26.39
November	18667689	205079	33996899	1210.42	110914.53	17.95	55.86	26.20
December	18865537	215268	36104486	1239.13	111321.90	17.89	56.16	25.94
January	19037109	211453	36997354	1218.37	113586.08	17.90	56.29	25.80
February	19235148	199523	32921958	1174.06	101035.98	17.90	56.44	25.66
March	19554297	225770	35616482	1492.76	111217.38	17.77	56.89	25.32
April	19570280	228604	37560980	1327.50	124182.49	17.78	56.88	25.33
May	19583234	229053	31212304	1340.73	123809.01	17.69	56.99	25.32

Source: RBI, Report on Trend and Progress of banking in India, 2012.

It is evident from the table that there has been an upward trend in number of transactions and amount of transactions through credit cards both at ATM and POS. Private Sector has been continuously dominating the share in total number of credit cards followed by foreign banks and Public sector banks. Progress of debit card number of transactions and amount of transactions for the period of August, 2012-May 2013 has been shown in Table 1.7

Table: 1.7
Progress in Debit card Number of Transactions and Amount of Transactions (August, 2012- May 2013)

Month	No of Debit cards	No. of Transactions (Actual)		Amount of transactions (Rs Million)		Percentage share in total number of Debit cards		
		ATM	POS	ATM	POS	Public Sector Banks	Private sector Banks	Foreign Sector Banks
August	298572426	445887954	38213667	1325727.71	58894.81	77.60	21.14	1.26
September	302481807	443969310	36915455	1306746.12	56436.56	77.61	21.15	1.25
October	306833366	468230840	39886107	1416358.04	67793.78	77.97	20.78	1.24
November	309477518	452153825	47117691	1452074.27	72201.10	77.84	20.91	1.24
December	314436803	473754492	43394716	1461246.93	69093.66	78.08	20.84	1.07
January	319970675	476637271	43530467	1491838.30	80057.20	78.09	20.85	1.04
February	325651757	452830692	40955500	1392833.90	61196.40	78.21	20.75	1.03
March	331196720	508849611	45672370	1556152.50	66940.30	78.67	20.32	1.01
April	336866879	501070235	45656423	1563868.50	76256.20	78.72	20.28	.99
May	341797185	514009166	47247141	1636134.18	76907.36	79.00	20.00	1.00

Source: RBI, Report on Trend and Progress of banking in India, 2012.

Above table depicts that there has been an upward trend in number of transactions and amount of transactions of debit cards both at ATM and POS. Public sector banks have been continuously dominating the share in total number of debit cards followed by private banks and foreign banks.

1.2 NEED OF THE STUDY

'E-banking' has attracted the considerable amount of interest of researchers in the recent times. Majority of the studies conducted in this field, primarily, focused on the identification of factors affecting the adoption of e-Banking services i.e. ATMs, Internet Banking, Mobile banking, phone Banking, ECS, Credit/debit Cards, RTGS, NEFT etc. Review of various studies has revealed that 'reliability', 'ease of use', 'personality', 'accessibility', 'accuracy', 'security' and 'efficiency' could influence the adoption of e-banking services (Joseph et. al., 1999; Meuter et al., 2000; Yang & Jun, 2002; Joseph & Sone, 2003; Long & McMellon, 2004). However, number of studies found that concern for 'security and privacy' is the most important factor influencing the adoption of e-banking (Polatoglu & Kin, 2001; Devlin & Young, 2003, Srivastava, 2007). The concern for security and privacy issues in adoption of internet banking is justifiable from the fact that according to Reserve Bank of India (RBI), in 2010-2011, Indian banks lost about Rs 2,289 Cr. in bank frauds while the loss in 2007-2008 was Rs 1,057 Cr (Jagdish Mahapatra, 2012) Similarly, according to the annual report of the Indian Computer Emergency Response Team (CERT-In), the team handled about 374 phishing incidents in 2009 ((Jagdish Mahapatra , 2012). A recent study conducted by PwC (2012) found that data security concerns and lack of clarity on regulatory stance are two major roadblocks in the adoption of internet banking (Cloud Computing) in Indian banks. Therefore, it is evident that with electronic banking on the rise, customers are vulnerable to the risks of e-banking frauds, even as regulations are becoming more stringent as far as know your customer (KYC) rules are concerned

In this background, it is apparent that concern for 'security and privacy' is the major roadblock in the adoption of e-banking services. So, there is a need to study the

security and privacy issues in depth from customers' perspective. An analysis of security features of online banking portals will help the bankers to make their online portals more secure by embedding the advanced security and privacy features in their online portals. Along with the study of online portals, the opinion of e-banking services users toward the security and privacy issues will help bankers to understand customers' concern for security and privacy while using e-banking services. Hence, the present study has been designed to study the security and privacy issues in e-banking by analyzing the contents of selected internet banking portals and the opinions of users of e-banking services.

1.3 OBJECTIVES OF THE STUDY

The specific objectives of the present study present study are;

1. To study the present status of e-banking services in India with respect to ATMs, Internet Banking, Mobile Banking, Credit Cards and Non-cash retail payments.
2. To study the security & privacy issues and regulatory environment of e-banking services in India.
3. To examine and compare the Pre-login and Post-login security and privacy features of selected banks' online banking portals.
4. To measure and compare the level of security and privacy concern among customers of selected banks regarding the use of e-banking services.
5. To measure and compare the level of security and privacy satisfaction among customers of selected banks regarding use of e-banking services.
6. To find out the relationship between security & privacy concern and security & privacy satisfaction.
7. To understand the opinion of non-users of e-banking services.

1.4 HYPOTHESIS OF THE STUDY

On the basis of objectives following Null hypotheses have been framed for testing purpose**:**

$H_0$1= There is no significant difference in the bank customers' perception towards security and privacy concern regarding use of ATMs across selected banks.

$H_0$2= There is no significant difference in the bank customers' perception towards security and privacy satisfaction regarding use of ATMs across selected banks.

$H_0$3= There is no relationship between bank customers' perception of 'security &privacy concern' and 'security & privacy satisfaction' in case of ATM use.

$H_0$4= There is no significant difference in bank customers' perception towards security and privacy concern regarding use of Internet Banking across selected banks.

$H_0$5= There is no significant difference in bank customers' perception towards security and privacy satisfaction regarding use of Internet Banking across selected banks.

$H_0$6= There is no relationship between bank customers' perception of 'security &privacy concern' and 'security & privacy satisfaction' in case of Internet banking use.

$H_0$7= There is no significant difference in the bank customers' perception towards security and privacy concern regarding use of Mobile Banking across selected banks.

$H_0$8= There is no significant difference in the bank customers' perception towards security and privacy satisfaction regarding use of Mobile Banking across selected banks.

$H_0$9= There is no relationship between bank customers' perception of 'security &privacy concern' and 'security & privacy satisfaction' in case of Mobile Banking use.

$H_0$10= There is no relationship between bank customers' perception of 'security &privacy concern' and 'security & privacy satisfaction' in case of Credit Cards use.

1.5 CHAPTER SCHEME

The present study has been divided into Six Chapters

Chapter 1: Introdcution

This chapter is introductory in nature. It discusses the present status of e-banking services in India with respect to ATMs, Internet Banking, Mobile Banking, Credit Cards and Non-cash retail payments. Further, need of the study has been discussed here along with objectives and hypotheses of the study.

Chapter 2 : Securtiy and Privacy Issues in E-Banking: Regulatory Environment

This chapter primarily focuses on Reserve Bank of India' s guidelines issued to commercial banks with respect to security and privacy of Internet Banking, ATMs, Mobile Banking, debit cards, Credit Cards etc. This chapter presents the brief picture of regulatory environment of e-banking in India.

Chapter 3: Review of Literature

This chapter deals with review of literature**.** In this chapter, important studies relating to adoption of e-banking services, perception towards quality of e-banking services, security and privacy issues in e-banking have been reviewed. Reviews studies are from India as well abroad.

Chapter 4: Research Methodology

This chapter gives the outline of research methodology used in the present study.

Chapter 5 Security and Privacy Issues in E-Banking: Content Analysis of Online Portals and Perception of Bank Customers

This chapter presents the analysis of customers' perception about security and privacy issues in banks, comparison of selected online portals, and perception of non users of e-banking services.

Chapter 6: Summary, Findings, Conclusion and Suggestions

This paper highlights the major findings that have been emerged from the study. This chapter also includes the implication of the study and suggestions made by the researcher to the banks.

Chapter – 2

SECURTIY AND PRIVACY ISSUES IN E-BANKING : REGULATORY ENVIRONMENT

During the past decade, a significant change has been observed in the way, the banking and financial organisations condcut transactions and offer product and servcies to their customers. The major reason behind such change has primarly been attributed to the application of Information and technology in the core functions of business. The extensive use of information technology by banks has put them under the pressure to provide confidentiality and integrity of information to maintain competitive edge, cash-flow, profitability, legal compliance and commercial image. However, information systems and the networks of the banking organisations have been facing security threats from a wide range of sources including computer-assisted fraud, espionage, sabotage, vandalism etc. The sources of damage such as the computer viruses, computer hacking and denial of service attacks have become more common, more ambitious and increasingly sophisticated in the networked environment. The ever-growing dependence of organisations on the information systems has made them more vulnerable to such security threats. This has made it imperative for each bank to put in place adequate security controls to ensure data accessibility to all the authorized users, data inaccessibility to all the unauthorized users, maintenance of data integrity and implementation of safeguards against all security threats to guarantee information and information systems security across the organization. In the light of above, the present chapter presents the overview of security and privacy risks in e-banking services and discusses the regulatory environment concerning security and privacy of e-banking.

2.1 SECURITY AND PRIVACY RISKS IN E-BANKING SERVICES

2.1.1 Security and Privacy Threats in ATM

The Automatic Teller Machine (ATM) was first commercially introduced in the 1960s. According to estimates by Retail Banking Research, there are **2,249,497 ATM worldwide and expected to increase to** 3,195,880 by end 2016 (Diebold).The introduction of the ATM proved to be an important technological development that enabled financial institutions to provide services to their customers in a 24X7 environment. The ATM has enhanced the convenience of customers by enabling them to access their cash wherever required from the nearest ATM. However, as the banker and the customer are not face-to-face, there is the risk of fraud, which may affect the customers and also the bank's reputation. ATM fraud is not confined to particular regions of the world. According to the white paper published by Diebold ATM threats can be segmented into three types of attacks: card and currency fraud, logical attacks and physical attacks.

Card and currency fraud

Card and currency fraud may take place through both direct attacks to steal cash from the ATM and indirect attacks to steal a consumer's identity (in the form of consumer card data and PIN theft). The purpose of indirect attacks is to fraudulently use the consumer data to create counterfeit cards and obtain money from the consumer's account through fraudulent redemption. Brief description of card and currency frauds is given below:

Skimming

These days, ATM card skimming is the most common and well known attack against ATMs. Card skimmers are devices used by fraudsters to capture cardholder data from the magnetic stripe on the back of an ATM card. These sophisticated devices, which are smaller than a deck of cards and resembling a hand-held credit card scanner, are often installed inside or over top of an ATM's originally installed card reader. When the consumer inserts his card into the card reader, the skimmer captures the card information before it passes into the ATMs card reader to initiate the transaction. When removed from the ATM, a skimmer allows the download of personal data belonging to everyone who used the ATM. Following are three kinds of card skimming attacks that can occur

i) External card skimming: placing a device over the card reader slot (motorized or dip) to capture consumer data from the magnetic stripe on the card during a transaction. This is the most common form of card skimming.

ii) Internal card skimming: gaining access to the top hat of the ATM to modify the card reader or replace the original card reader with an already modified one for the purpose of obtaining consumer card data during a transaction.

iii) Vestibule card skimming: in locations where the ATM is located within a vestibule, skimmers are placed on the vestibule door card access reader to capture cardholder data from the magnetic stripe where the card is read so an unwary consumer inserts their card into the vestibule instead of on the ATM.

Fraudsters usually combine skimming attack with other fraudulent devices such as covert cameras or keypad overlays that capture the consumer's PIN as it is being entered on the keypad during a transaction. Sometimes, fraudsters even install signs on ATMs instructing cardholders to "swipe here first" before continuing with transactions. Another fraudulent method is to portray the additional card reader as a "card cleaner" designed to extend the life and improve the performance of ATM magnetic stripes.

Card Trapping/Fishing

Card trapping and fishing attempt to steal consumers' cards itself rather than information on it. It takes place when card is inserted into the card reader during a transaction. The purpose of this type of attack is to steal the card and use it at a later time to make fraudulent withdrawals from the consumers' accounts. Card trapping is conducted by placing a device over or inside the card reader slot to capture the consumer's card. These can be devices such as plates over the card reader, thin metallic strips covered in a plastic transparent film, wires, probes and hooks. These devices are designed to prevent the card from being returned to the consumer at the end of a transaction. These attacks are sometimes combined with other fraudulent devices such as cameras or keypad overlays to capture the consumer's PIN as it is being entered on the keypad during a transaction.

Currency Trapping/Fishing

Currency trapping and fishing is an attempt by perpetrators to capture currency that is dispensed by the ATM during a transaction. 'Trapping' takes place when a false dispenser front is placed over the shutter of the dispenser with adhesive or tape on the inside to trap the notes before they are dispensed. Currency Fishing takes place by using the methods which are similar to those used to fish for cards.

Wires, probes and hooks that are difficult for the consumer to see are used to prevent cash from being dispensed or deposits from being made. When the unwary consumer leaves the ATM, the perpetrator returns and uses the fishing device to retrieve the currency or deposit envelope.

Logical/data Attacks

Logical attacks target an ATM's software, operating system and communications systems. Logical attacks can be some of the most damaging in terms of the quantity of consumer data compromised. The migration from proprietary operating systems to Microsoft Windows® technology has led to greater connectivity and interconnectivity of ATMs. Vast networks—including ATMs, branch systems, phone systems and other infrastructure connected via the Internet—are targets of logical security threats. Logical attackers include vandals who author viruses intended to exploit an ATM's operating system and hackers who install malware to violate the confidentiality, integrity or authenticity of transaction-related data.

Malware and Hacking

With any computer system, the purpose of installing malicious software (malware) is to violate the confidentiality, integrity and/or authenticity of data on that computer system. These are designed to collect cardholders' data and/or dispense cash, malware and hacking can occur both locally or remotely. Local attacks operate by accessing the top hat and downloading the malware using a USB drive or attaching a USB sniffing device to intercept communication between the card reader and the ATM's computer. Remote attacks on an ATM network occur at some point in the communication with the host or at the backend infrastructure. Typically, these sophisticated attacks are carried out by well-funded criminal organizations. Malware

threats are of particular concern as they are on the rise and constantly evolving in an attempt to stay ahead of security measures.

Physical Attacks

Physical attacks on an ATM include any type of assault that physically damages the components of the ATM in an attempt to obtain cash. While the entire ATM can be a target for a physical attack, specific components of the ATM are often targeted. Specific component, which may be targeted are Safe, Top Hat, Presenter and Depositor. Ramming, Pulling and Lifting are used to remove the entire ATM.

2.1.2 Security and Privacy threats in Internet Banking:

When the internet was developed, the founding fathers of internet hardly had any inclination that internet could also be misused for criminal activities. Since the beginning of the year 2004, reports of fraud cases nearly explode especially in internet banking. Major internet banking threats have been discusses as under:

Phishing Attacks

Phishing is an attempt by fraudsters to 'fish' for banking details of customers. A phishing attempt usually is in the form of an e-mail that appears to be from customer's bank. The e-mail usually encourages customer to click a link in it that takes him to a fraudulent log-on page designed to capture authentication details such as password and Login ID. E-mail addresses can be obtained from publicly available sources or through randomly generated lists. Here is the example[3] of phishing Attack mail

[3] http://www.icicibank.com/online-safe-banking/phishing-mail2.html

Spoofing

Website spoofing is the act of creating a website, as a hoax, with the intention of performing fraud. To make spoof sites seem legitimate, phishers use the names, logos, graphics and even code of the actual website. They can even fake the URL that appears in the address field at the top of your browser window and the Padlock icon that appears at the bottom right corner.

Vishing

Vishing is a combination of Voice and Phishing that uses Voice over Internet Protocol (VoIP) technology wherein fraudsters feigning to represent real companies such as banks attempt to trick unsuspecting customers into providing their personal and financial details over the phone.

Further Malware, Viruses, Trojans, Key-loggers, Spywares etc are common methods of identity theft used by fraudsters in case of internet banking.

2.1.3 Security and Privacy threats in Mobile Banking:

Almost similar techniques which are being used by fraudster in internet banking are being used in mobile banking for identity theft.

2.1.4 Security and Privacy threats in Credit cards

Credit cards frauds can be broadly classified into three categories[4], i.e., Card related frauds, Merchant related frauds and Internet frauds. The different types of methods for committing credit card frauds are described below:

Card Related Frauds

Application Fraud

This type of fraud occurs when a person falsifies an application to acquire a credit card. Application fraud can be committed in three ways: *Assumed identity*: where an individual illegally obtains personal information of another individual and opens accounts in his or her name, using partially legitimate information. *Financial fraud*: where an individual provides false information about his or her financial status to acquire credit. *Not-received items (NRIs):* also called postal intercepts occur when a card is stolen from the postal service before it reaches its owner's destination

Lost/ stolen cards

A card is lost/stolen when a legitimate account holder receives a card and loses it or someone steals the card for criminal purposes. This type of fraud is in essence the easiest way for a fraudster to get hold of other individual's credit cards without investment in technology.

Counterfeit cards

The creation of counterfeit cards, together with lost / stolen cards poses highest threat in credit card frauds. Some of the techniques used for creating false and

[4] Bhatla, Prabhu and Dua ,2003.

counterfeit cards are erasing the magnetic strip, Creating a fake card, Altering card details, Skimming, White plastic etc

Merchant Related Frauds

Merchant related frauds are initiated either by owners of the merchant establishment or their employees. The types of frauds initiated by merchants are described below:

Merchant collusion

This type of fraud occurs when merchant owners and/or their employees conspire to commit fraud using their customers' (cardholder) accounts and/or personal information.

Triangulation

The fraudster in this type of fraud operates from a fake web site. Goods are offered at heavily discounted rates and are also shipped before payment. The customer while placing orders online provides information such as name, address and valid credit card details to the site. Once fraudsters receive these details, they order goods from a legitimate site using stolen credit card details.

Internet Related Frauds

The most commonly used techniques in internet fraud are described below:

Site cloning: Site cloning is where fraudsters clone an entire site or just the pages from which order is placed. The consumer suspects nothing, whilst the fraudsters have all the details they need to commit credit card fraud.

False merchant sites: These sites often offer the customer an extremely cheap service. The site requests a customer's complete credit card details such as name and address in return for access to the content of the site. Most of these sites claim to be free, but require a valid credit card number to verify an individual's age. These sites

are set up to accumulate as many credit card numbers as possible. The sites themselves never charge individuals for the services they provide. The sites are usually part of a larger criminal network that either uses the details it collects to raise revenues or sells valid credit card details to small fraudsters.

Credit card generators: Credit card number generators are computer programs that generate valid credit card numbers and expiry dates. These generators work by generating lists of credit card account numbers from a single account number. The software works by using the mathematical Luhn algorithm that card issuers use to generate other valid card number combinations. The generators allow users to illegally generate as many numbers as the user desires, in the form of any of the credit card formats, whether it be American Express, Visa or MasterCard.

2.2 SECURITY AND PRIVACY REGULATORY ENVIRONMENT

The part primarily focuses on Reserve Bank of India's guidelines issued from to commercial banks with respect to security and privacy of Internet Banking, ATMs, Mobile Banking, and Credit Cards etc.

2.2.1 Security and Privacy regulatory environment: Internet Banking

Internet banking is a popular and convenient method of doing online banking transactions but there is no dedicated Internet banking laws in India. However, Reserve Bank of India (RBI) has been consistently making efforts to bring more make internet banking transactions more and more secure. During the year 2010, Reserve Bank of India set up a Working Group under the Chairmanship of S.R Mittal to address the Regulatory and Supervisory concerns in i-banking focusing on i) Legal and regulatory issues, (ii) Security and technology issues and (iii) Supervisory and

operational issues. Major recommendations of the Group accepted by RBI have been listed as under.[5]

I. Technology and Security Standards:

a. Banks should designate a network and database administrator who will ensure that only the latest versions of the licensed software with latest patches are installed in the system, proper user groups with access privileges are created and users are assigned to appropriate groups as per their business roles, a proper system of back up of data and software is in place and is strictly adhered to, business continuity plan is in place and frequently tested and there is a robust system of keeping log of all network activity and analyzing the same. **(Para 6.2.4)**

b. Banks should have a security policy duly approved by the Board of Directors. There should be a segregation of duty of Security Officer / Group dealing exclusively with information systems security and Information Technology Division which actually implements the computer systems. Further, Information Systems Auditor will audit the information systems. **(Para 6.3.10, 6.4.1)**

c. Banks should introduce logical access controls to data, systems, application software, utilities, telecommunication lines, libraries, system software, etc. Logical access control techniques may include user-ids, passwords, smart cards or other biometric technologies. **(Para 6.4.2)**

d. At the minimum, banks should use the proxy server type of firewall so that there is no direct connection between the Internet and the bank's system. It facilitates a high level of control and in-depth monitoring using logging and

[5] Vide RBI Circular, DBOD.COMP.BC.No.130/ 07.03.23/ 2000-01, June 14, 2001.

auditing tools. For sensitive systems, a stateful inspection firewall is recommended which thoroughly inspects all packets of information, and past and present transactions are compared. These generally include a real time security alert. **(Para 6.4.3)**

e. All the systems supporting dial up services through modem on the same LAN as the application server should be isolated to prevent intrusions into the network as this may bypass the proxy server. **(Para 6.4.4)**

f. PKI (Public Key Infrastructure) is the most favoured technology for secure Internet banking services. However, as it is not yet commonly available, banks should use the following alternative system during the transition, until the PKI is put in place:

    1. Usage of SSL (Secured Socket Layer), which ensures server authentication and use of client side certificates issued by the banks themselves using a Certificate Server.
    2. The use of at least 128-bit SSL for securing browser to web server communications and, in addition, encryption of sensitive data like passwords in transit within the enterprise itself. (Para 6.4.5)

g. It is also recommended that all unnecessary services on the application server such as FTP (File Transfer Protocol), telnet should be disabled. The application server should be isolated from the e-mail server. **(Para 6.4.6)**

h. All computer accesses, including messages received, should be logged. Security violations (suspected or attempted) should be reported and follow up action taken should be kept in mind while framing future policy. Banks should acquire tools for monitoring systems and the networks against intrusions and attacks. These tools should be used regularly to avoid security breaches. The

banks should review their security infrastructure and security policies regularly and optimize them in the light of their own experiences and changing technologies. They should educate their security personnel and also the end-users on a continuous basis. **(Para 6.4.7, 6.4.11, 6.4.12)**

i. The information security officer and the information system auditor should undertake periodic penetration tests of the system, which should include:
    1. Attempting to guess passwords using password-cracking tools.
    2. Search for back door traps in the programs.
    3. Attempt to overload the system using DDoS (Distributed Denial of Service) & DoS (Denial of Service) attacks.
    4. Check if commonly known holes in the software, especially the browser and the e-mail software exist.
    5. The penetration testing may also be carried out by engaging outside experts (often called 'Ethical Hackers'). **(Para 6.4.8)**

j. Physical access controls should be strictly enforced. Physical security should cover all the information systems and sites where they are housed, both against internal and external threats. **(Para 6.4.9)**

k. Banks should have proper infrastructure and schedules for backing up data. The backed-up data should be periodically tested to ensure recovery without loss of transactions in a time frame as given out in the bank's security policy. Business continuity should be ensured by setting up disaster recovery sites. These facilities should also be tested periodically. **(Para 6.4.10)**

l. All applications of banks should have proper record keeping facilities for legal purposes. It may be necessary to keep all received and sent messages both in encrypted and decrypted form. **(Para 6.4.13)**

m. Security infrastructure should be properly tested before using the systems and applications for normal operations. Banks should upgrade the systems by installing patches released by developers to remove bugs and loopholes, and upgrade to newer versions which give better security and control. **(Para 6.4.15)**

II. Legal Issues

a. Considering the legal position prevalent, there is an obligation on the part of banks not only to establish the identity but also to make enquiries about integrity and reputation of the prospective customer. Therefore, even though request for opening account can be accepted over Internet, accounts should be opened only after proper introduction and physical verification of the identity of the customer. **(Para 7.2.1)**

b. From a legal perspective, security procedure adopted by banks for authenticating users needs to be recognized by law as a substitute for signature. In India, the Information Technology Act, 2000, in Section 3(2) provides for a particular technology (viz., the asymmetric crypto system and hash function) as a means of authenticating electronic record. Any other method used by banks for authentication should be recognized as a source of legal risk.**(Para 7.3.1)**

c. Under the present regime there is an obligation on banks to maintain secrecy and confidentiality of customers' accounts. In the Internet banking scenario, the risk of banks not meeting the above obligation is high on account of several factors. Despite all reasonable precautions, banks may be exposed to enhanced risk of liability to customers on account of breach of secrecy, denial of service etc., because of hacking/ other technological failures. The banks

should, therefore, institute adequate risk control measures to manage such risks. **(Para 7.5.1-7.5.4)**

d. In Internet banking scenario there is very little scope for the banks to act on stop-payment instructions from the customers. Hence, banks should clearly notify to the customers the timeframe and the circumstances in which any stop-payment instructions could be accepted. **(Para 7.6.1)**

e. The Consumer Protection Act, 1986 defines the rights of consumers in India and is applicable to banking services as well. Currently, the rights and liabilities of customers availing of Internet banking services are being determined by bilateral agreements between the banks and customers. Considering the banking practice and rights enjoyed by customers in traditional banking, banks' liability to the customers on account of unauthorized transfer through hacking, denial of service on account of technological failure etc. needs to be assessed and banks providing Internet banking should insure themselves against such risks**. (Para 7.11.1)**

III. Regulatory and Supervisory Issues:

As recommended by the Group, the existing regulatory framework over banks will be extended to Internet banking also. In this regard, it is advised that:

1. Only such banks which are licensed and supervised in India and have a physical presence in India will be permitted to offer Internet banking products to residents of India. Thus, both banks and virtual banks incorporated outside the country and having no physical presence in India will not, for the present, be permitted to offer Internet banking services to Indian residents.
2. The products should be restricted to account holders only and should not be offered in other jurisdictions.

3. The services should only include local currency products.
4. The 'in-out' scenario where customers in cross border jurisdictions are offered banking services by Indian banks (or branches of foreign banks in India) and the 'out-in' scenario where Indian residents are offered banking services by banks operating in cross-border jurisdictions are generally not permitted and this approach will apply to Internet banking also. The existing exceptions for limited purposes under FEMA i.e. where resident Indians have been permitted to continue to maintain their accounts with overseas banks etc., will, however, be permitted.
5. Overseas branches of Indian banks will be permitted to offer Internet banking services to their overseas customers subject to their satisfying, in addition to the host supervisor, the home supervisor.

Given the regulatory approach, RBI advised banks to follow the following instructions:

a. All banks, who propose to offer transactional services on the Internet should obtain prior approval from RBI. Bank's application for such permission should indicate its business plan, analysis of cost and benefit, operational arrangements like technology adopted, business partners, third party service providers and systems and control procedures the bank proposes to adopt for managing risks. The bank should also submit a security policy covering recommendations made in this circular and a certificate from an independent auditor that the minimum requirements prescribed have been met. After the initial approval the banks will be obliged to inform RBI any material changes in the services / products offered by them. **(Para 8.4.1, 8.4.2)**

b. Banks will report to RBI every breach or failure of security systems and procedure and the latter, at its discretion, may decide to commission special audit / inspection of such banks. **(Para 8.4.3)**

c. The guidelines issued by RBI on 'Risks and Controls in Computers and Telecommunications' vide circular DBS.CO.ITC.BC. 10/ 31.09.001/ 97-98 dated 4th February 1998 will equally apply to Internet banking. The RBI as supervisor will cover the entire risks associated with electronic banking as a part of its regular inspections of banks. **(Para 8.4.4, 8.4.5)**

d. Banks should develop outsourcing guidelines to manage risks arising out of third party service providers, such as, disruption in service, defective services and personnel of service providers gaining intimate knowledge of banks' systems and misutilizing the same, etc., effectively. **(Para 8.4.7)**

e. With the increasing popularity of e-commerce, it has become necessary to set up 'Inter-bank Payment Gateways' for settlement of such transactions. The protocol for transactions between the customer, the bank and the portal and the framework for setting up of payment gateways as recommended by the Group should be adopted. **(Para 8.4.7, 8.4.9.1 – 8.4.9.5)**

f. Only institutions who are members of the cheque clearing system in the country will be permitted to participate in Inter-bank payment gateways for Internet payment. Each gateway must nominate a bank as the clearing bank to settle all transactions. Payments effected using credit cards, payments arising out of cross border e-commerce transactions and all intra-bank payments (i.e., transactions involving only one bank) should be excluded for settlement through an inter-bank payment gateway. **(Para 8.4.7)**

g. Inter-bank payment gateways must have capabilities for both net and gross settlement. All settlement should be intra-day and as far as possible, in real time. **(Para 8.4.7)**

h. Connectivity between the gateway and the computer system of the member bank should be achieved using a leased line network (not through Internet) with appropriate data encryption standard. All transactions must be authenticated. Once, the regulatory framework is in place, the transactions should be digitally certified by any licensed certifying agency. SSL / 128 bit encryption must be used as minimum level of security. Reserve Bank may get the security of the entire infrastructure both at the payment gateway's end and the participating institutions' end certified prior to making the facility available for customers use. **(Para 8.4.7)**

i. Bilateral contracts between the payee and payees bank, the participating banks and service provider and the banks themselves will form the legal basis for such transactions. The rights and obligations of each party must be clearly defined and should be valid in a court of law. **(Para 8.4.7)**

j. Banks must make mandatory disclosures of risks, responsibilities and liabilities of the customers in doing business through Internet through a disclosure template. The banks should also provide their latest published financial results over the net. **(Para 8.4.8)**

k. Hyperlinks from banks' websites often raise the issue of reputational risk. Such links should not mislead the customers into believing that banks sponsor any particular product or any business unrelated to banking. Hyperlinks from a banks' websites should be confined to only those portals with which they have a payment arrangement or sites of their subsidiaries or principals. Hyperlinks

to banks' websites from other portals are normally meant for passing on information relating to purchases made by banks' customers in the portal. Banks must follow the minimum recommended security precautions while dealing with request received from other websites, relating to customers' purchases. **(Para 8.4.9)**

As per revised guidelines[6]no prior approval of the Reserve Bank of India will be required for offering Internet Banking services.

Further, The Working Group on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds (2010) was constituted, under the Chairmanship of Shri G. Gopalakrishna, Executive Director, RBI. The Group examined various issues arising out of the use of Information Technology in banks and made its recommendations in nine broad areas. These areas were **IT Governance, Information Security, IS Audit, IT Operations, IT Services Outsourcing, Cyber Fraud, Business Continuity Planning, Customer Awareness programmes and Legal aspects.** Final guidelines[7] in the respective areas as mentioned above were issued to banks for implementation. Important guidelines with respect to security of internet banking are reproduced here.

Authentication practices for internet banking:

1. Authentication methodologies may involve three basic "factors" of securities :
    a. Something the user knows (e.g., password, PIN);
    b. Something the user has (e.g., ATM card, smart card); and
    c. Something the user is (e.g., biometric characteristic, such as a fingerprint).

6 RBI/2005-06/71 DBOD No. Comp.BC.14/07.03.29/2005-06, July 2005.
7 RBI/2010-11/494, DBS.CO.ITC.BC.No. 6/31.02.008/2010-11, April 29, 2011.

2. Properly designed and implemented multifactor authentication methods are more reliable and stronger fraud deterrents and are more difficult to compromise. The principal objectives of two-factor authentication are to protect the confidentiality of customer account data and transaction details as well as enhance confidence in internet banking by combating various cyber attack mechanisms like phishing, key-logging, spyware-malware and other internet based frauds targeted at banks and their customers.

Implementation of two-factor authentication and other security measures for internet banking:

1. In view of the proliferation of cyber attacks and their potential consequences, banks should implement two-factor authentication for fund transfers through internet banking.
2. The implementation of appropriate authentication methodologies should be based on an assessment of the risk posed by the institution's Internet banking systems. The risk should be evaluated in light of the type of customer (e.g., retail or corporate/ commercial); the customer transactional capabilities (e.g., bill payment, fund transfer), the sensitivity of customer information being communicated to both the bank and the volume of transactions involved.
3. Beyond the technology factor, the success of a particular authentication method depends on appropriate policies, procedures, and controls. An effective authentication method should take into consideration customer acceptance, ease of use, reliable performance, scalability to accommodate growth, and interoperability with other systems.

4. There is a legal risk in not using the asymmetric cryptosystem and hash function for authenticating electronic transactions. However, it is observed that some banks still use weak user id/password based authentication for fund transfers using internet banking. For carrying out critical transactions like fund transfers, the banks, at the least, need to implement robust and dynamic two-factor authentication through user id/password combination and second factor like (a) a digital signature (through a token containing digital certificate and associated private key) (preferably for the corporate customers) or (b) OTP/dynamic access code through various modes (like SMS over mobile phones or hardware token).
5. To enhance online processing security, confirmatory second channel procedures (like telephony, SMS, email etc) should be applied in respect of transactions above pre-set values, creation of new account linkages, registration of third party payee details, changing account details or revision to funds transfer limits. In devising these security features, the bank should take into account their efficacy and differing customer preferences for additional online protection.
6. Based on mutual authentication protocols, customers could also authenticate the bank's web site through security mechanisms such as personal assurance messages/images, exchange of challenge response security codes and/or the secure sockets layer (SSL) server certificate verification. In recent times, Extended Validation Secure Sockets Layer (EV-SSL) Certificates are increasingly being used. These are special SSL Certificates that work with high security Web browsers to clearly identify a Web site's organizational identity. It should, however, be noted that SSL is

only designed to encrypt data in transit at the network transport layer. It does not provide end-to-end encryption security at the application layer.

7. An authenticated session, together with its encryption protocol, should remain intact throughout the interaction with the customer. Else, in the event of interference, the session should be terminated and the affected transactions resolved or reversed out. The customer should be promptly notified of such an incident as the session is being concluded or subsequently by email, telephone or through other means.
8. Changes in mobile phone number may be done through request from a branch only.
9. Implementation of virtual keyboard.
10. A cooling period for beneficiary addition and SMS and E-mail alerts when new beneficiaries are added.
11. Customers should be advised to adopt various good security precautions and practices in protecting their personal computer and to avoid conducting financial transactions from public or internet café computers.
12. Risk based transaction monitoring or surveillance process needs to be considered as an adjunct.
13. An online session would need to be automatically terminated after a fixed period of time unless the customer is re-authenticated for the existing session to be maintained. This prevents an attacker from keeping an internet banking session alive indefinitely.
14. By definition true multifactor authentication requires the use of solutions from two or more of the three categories of factors. Using multiple solutions from the same category at different points in the process may be

part of a layered security or other compensating control approach, but it would not constitute a true multifactor authentication.

15. As an integral part of the two factor authentication architecture, banks should also implement appropriate measures to minimise exposure to a middleman attack which is more commonly known as a man-in-the-middle attack (MITM), man-in-the browser (MITB) attack or man-in-the application attack. The banks should also consider, and if deemed appropriate, implement the following control and security measures to minimise exposure to man-in-the middle attacks:

    a. **Specific OTPs for adding new payees**: Each new payee should be authorized by the customer based on an OTP from a second channel which also shows payee details or the customer's handwritten signature from a manual procedure which is verified by the bank.

    b. **Individual OTPs for value transactions (payments and fund transfers)**: Each value transaction or an approved list of value transactions above a certain rupee threshold determined by the customer should require a new OTP.

    c. **OTP time window**: Challenge-based and time-based OTPs provide strong security because their period of validity is controlled entirely by the bank and does not depend user behaviour. It is recommended that the banks should not allow the OTP time window to exceed 100 seconds on either side of the server time since the smaller the time window, the lower the risk of OTP misuse.

    d. **Payment and fund transfer security**: Digital signatures and key-based message authentication codes (KMAC) for payment or fund

transfer transactions could be considered for the detection of unauthorized modification or injection of transaction data in a middleman attack. For this security solution to work effectively, a customer using a hardware token would need to be able to distinguish the process of generating a one-time password from the process of digitally signing a transaction. What he signs digitally must also be meaningful to him, which means the token should at least explicitly show the payee account number and the payment amount from which a hash value may be derived for the purpose of creating a digital signature. Different crypto keys should be used for generating OTPs and for signing transactions.

e. **Second channel notification / confirmation**: The bank should notify the customer, through a second channel, of all payment or fund transfer transactions above a specified value determined by the customer.

f. **Session time-out:** An online session would be automatically terminated after a fixed period of time unless the customer is re-authenticated for the existing session to be maintained. This prevents an attacker from keeping an internet banking session alive indefinitely.

g. **SSL server certificate warning**: Internet banking customers should be made aware of and shown how to react to SSL or EV-SSL certificate warning.

Securing Electronic Payment Transactions

With the diffusion of internet banking, electronic modes of payment like RTGS, NEFT and IMPS have emerged as channels of funds transfer. Hence, it is important that such delivery channels would also be safe and secure. Recently, RBI has issued additional Security and Risk Mitigation measures for Electronic Payment Transactions[8] in this regard which are being reproduced as follows;

1. Customer induced options may be provided for fixing a cap on the value / mode of transactions/beneficiaries. In the event of customer wanting to exceed the cap, an additional authorization may be insisted upon.
2. Limit on the number of beneficiaries that may be added in a day per account could be considered.
3. A system of alert may be introduced when a beneficiary is added.
4. Banks may put in place mechanism for velocity check on the number of transactions effected per day/ per beneficiary and any suspicious operations should be subjected to alert within the bank and to the customer.
5. Introduction of additional factor of authentication (preferably dynamic in nature) for such payment transactions should be considered.
6. The banks may consider implementation of digital signature for large value payments for all customers, to start with for RTGS transactions.
7. Capturing of Internet Protocol (IP) address as an additional validation check should be considered.
8. Sub-membership of banks to the centralised payment systems has made it possible for the customers of such sub-members to reap the benefits of the same. Banks accepting sub-members should ensure that the security measures

[8] RBI / 2012 -13/424 , DPSS (CO) PD No.1462 / 02.14.003 / 2012-13 February 28, 2013.

put in place by the sub members are on par with the standards followed by them so as to ensure the safety and mitigate the reputation risk.

9. Banks may explore the feasibility of implementing new technologies like adaptive authentication, etc. for fraud detection.

The above security measures under B (i) to (ix) are expected to be put in place by banks by June 30, 2013.

2.2.2 Security and Privacy Regulatory Environment : ATM[9]

Based on a review of the developments and with a view to further improve the customer service through enhancement of efficiency in ATM operations, RBI advised banks to initiate action as below:

a. The message regarding non-availability of cash in ATMs should be displayed before the transaction is initiated by the customer. Banks may exercise option to display such notices either on screen or in some other way.

b. The ATM ID may be displayed clearly in the ATM premises to enable a customer to quote the same while making a complaint / suggestion.

c. Reiterating our earlier instructions, issued vide circulars, DPSS.CO.PD.2018/ 02.10.002/2009-10 dated March 19, 2010;DPSS.CO.PD.2359/02.10.002/2009-10 dated May 3, 2010, DPSS. No. 2753/02.10.02/2009-2010 dated June 15, 2010 and DPSS.CO.PD. No. 52/ 02.10.02/2010-2011 dated July 6, 2010, banks are advised to make available the forms for lodging ATM complaints within the ATM premises and also display the name and phone number of the officials with whom the complaint can be lodged. This will help in avoiding delays in lodging complaints.

[9] RBI/2013-14/171, DPSS.CO.PD.No. 289/02.10.002/2013-2014, August 1, 2013

d. Banks may make available sufficient toll-free phone numbers for lodging complaints / reporting and blocking lost cards to avoid delays and also attend the requests on priority. Local helpline numbers (city-wise / centre wise) should also be increased and should be prominently displayed in the ATM premises / banks' web-site.

e. Banks may proactively register the mobile numbers / e-mail IDs of their customers for sending alerts and also educate their customers to intimate changes, if any. A time-bound programme for updation of mobile number and or e-mail of all existing accounts may be drawn up. These details should be updated periodically along with KYC details.

f. To prevent fraudulent withdrawal at ATMs, RBI had mandated requirement of PIN entry for each and every transaction, including balance enquiry transactions. Banks already have in place time limits for completion of transactions at ATMs. However, as an additional safety measure, it is advised that the time out sessions should be enabled for all screens / stages of ATM transaction keeping in view the time required for such functions in normal course. Bank may ensure that no time extensions are allowed beyond a reasonable limit at any stage of the transaction.

g. Creating awareness about electronic banking products is of utmost importance to prevent frauds taking place in this field and also to make customers aware of their rights and responsibilities. In view of changes taking place in this field, banks, in collaboration with Indian Banks' Association, may run advertisement campaign in both, print and electronic media at regular intervals

2.2.3 Security and Privacy Regulatory Environment in Mobile Banking

The rapid growth of mobile users in India, through wider coverage of mobile phone networks, have made this medium an important platform for extending banking services to every segment of banking clientele in general and the unbanked segment in particular. In order to ensure a level playing field and considering that the technology is relatively new, Reserve Bank brought out a set of operating guidelines[10] for adoption by banks. Security related guidelines depicted in various circulars[11] are reproduced as under:

1. Technology used for mobile banking must be secure and should ensure confidentiality, integrity, authenticity and non-repudiability.
2. Transactions up to Rs 5000/- can be facilitated by banks without end-to-end encryption. The risk aspects involved in such transactions may be addressed by the banks through adequate security measures.
3. Banks are permitted to offer mobile banking facility to their customers without any daily cap for transactions involving purchase of goods/services. However, banks may put in place per transaction limit depending on the bank's own risk perception, with the approval of its Board.
4. Banks are required to put in place appropriate risk mitigation measures like transaction limit (per transaction, daily, weekly, monthly), transaction velocity limit, fraud checks, AML checks etc. depending on the bank's own risk perception, unless otherwise mandated by the Reserve Bank.

---

10 RBI/2013-14/116 DPSS.CO.PD. Mobile Banking. No./02.23.001/2013-14 July 1, 2013.

11 DPSS.CO.No.619 /02.23.02/ 2008-09, DPSS.CO.No.1357/02.23.02/ 2009-10, DPSS.CO.No.2502 /02.23.02/ 2010 11, DPSS.PD.CO.No. 62/ 02.27.019 / 2011-2012, DPSS.CO.PD.No. 1098 / 02.23.02 / 2011-12.

5. **Authentication :** Banks providing mobile banking services shall comply with the following security principles and practices for the authentication of mobile banking transactions:
    a. All mobile banking transactions shall be permitted only by validation through a two factor authentication.
    b. One of the factors of authentication shall be mPIN or any higher standard.
    c. Where mPIN is used, end to end encryption of the mPIN is desirable, i.e. mPIN shall not be in clear text anywhere in the network.
    d. The mPIN shall be stored in a secure environment.
6. **Encryption and security**: Proper level of encryption and security shall be implemented at all stages of the transaction processing. The endeavor shall be to ensure end-to-end encryption of the mobile banking transaction. Adequate safe guards would also be put in place to guard against the use of mobile banking in money laundering, frauds etc. The following guidelines with respect to network and system security shall be adhered to:
    a. Implement application level encryption over network and transport layer encryption wherever possible.
    b. Establish proper firewalls, intruder detection systems (IDS), data file and system integrity checking, surveillance and incident response procedures and containment procedures.
    c. Conduct periodic risk management analysis, security vulnerability assessment of the application and network etc at least once in a year
    d. Maintain proper and full documentation of security practices, guidelines, methods and procedures used in mobile banking and

payment systems and keep them up to date based on the periodic risk management, analysis and vulnerability assessment carried out.

e. Implement appropriate physical security measures to protect the system gateways, network equipments, servers, host computers, and other hardware/software used from unauthorized access and tampering. The Data Centre of the Bank and Service Providers should have proper wired and wireless data network protection mechanism.

2.2.4 Security and Privacy Regulatory Environment : Credit cards

The quality of banks' credit card portfolios mirrors the economic environment in which they operate. Very often, there is a strong correlation between an economic downturn and deterioration in the quality of such portfolios. The deterioration may become even more serious if banks have relaxed their credit underwriting criteria and risk management standards as a result of intense competition in the market. It is therefore important for banks to maintain prudent policies and practices for managing the risks of their credit card business which are relevant to the market environment that they operate in. In this background, RBI issued latest guidelines[12] with respect to operation of credit cards. Security and privacy related important guidelines are reproduced here.

Customer confidentiality

a. The card issuing bank/NBFC should not reveal any information relating to customers obtained at the time of opening the account or issuing the credit card to any other person or organization without obtaining their specific consent, as regards the purpose/s for which the information will be used and the organizations with whom the information will be shared.

[12] RBI/2013-14/60, DBOD.No.FSD.BC. 4/24.01.011/2013-14, July 1, 2013.

b. Instances have come to light where banks, as part of the MITCs, obtain the consent of the customer for sharing the information furnished by him while applying for the credit card, with other agencies. Banks should give the customer the option to decide as to whether he is agreeable for the bank sharing with other agencies the information furnished by him at the time of applying for credit card. The application form for credit card may be suitably modified to explicitly provide for the same.

c. Further, in case where the customers gives his consent for the bank sharing the information with other agencies, banks should explicitly state and explain clearly to the customer the full meaning/ implications of the disclosure clause. Banks/NBFCs should satisfy themselves, based on specific legal advice, that the information being sought from them is not of such nature as will violate the provisions of the laws relating to secrecy in the transactions. Banks/ NBFCs would be solely responsible for the correctness or otherwise of the data provided for the purpose.

d. In case of providing information relating to credit history / repayment record of the card holder to a credit information company (specifically authorized by RBI), the bank/NBFC may explicitly bring to the notice of the customer that such information is being provided in terms of the Credit Information Companies (Regulation) Act, 2005.

e. Before reporting default status of a credit card holder to a Credit Information Company which has obtained Certificate of Registration from RBI and of which the bank / NBFC is a member, banks/NBFCs should ensure that they adhere to a procedure, duly approved by their Board, including issuing of sufficient notice to such card holder about the intention to report him/ her as

defaulter to the Credit Information Company. The procedure should also cover the notice period for such reporting as also the period within which such report will be withdrawn in the event the customer settles his dues after having been reported as defaulter. Banks /NBFCs should be particularly careful in the case of cards where there are pending disputes. The disclosure/ release of information, particularly about the default, should be made only after the dispute is settled as far as possible. In all cases, a well laid down procedure should be transparently followed. These procedures should also be transparently made known as part of MITCs.

f. The disclosure to the DSAs / recovery agents should also be limited to the extent that will enable them to discharge their duties. Personal information provided by the card holder but not required for recovery purposes should not be released by the card issuing bank/NBFC. The card issuing bank /NBFCs should ensure that the DSAs / DMAs do not transfer or misuse any customer information during marketing of credit card products

Fraud Control

1. Banks/NBFCs should set up internal control systems to combat frauds and actively participate in fraud prevention committees/ task forces which formulate laws to prevent frauds and take proactive fraud control and enforcement measures.
2. With a view to reducing the instances of misuse of lost/stolen cards, it is recommended to banks/NBFCs that they may consider issuing (i) cards with photographs of the cardholder (ii) cards with PIN and (iii) signature laminated cards or any other advanced methods that may evolve from time to time.

3. In terms of instructions issued by Department of Payment and Settlement Systems, Reserve Bank of India on security issues and risk mitigation measures, as amended from time to time, banks have been advised to put in place a system of providing for additional authentication/ validation based on information not visible on the cards. The same has been extended to Mail order Transactions Order (MOTO) transactions, which are also a subset of the card-not present transactions. Further, banks have been advised to take steps to put in place a system of online alerts for all types of transactions irrespective of the amount, involving the usage of cards at various channels. Banks have also been advised to put in place various security and risk mitigation measures for electronic payment transactions, in terms of guidelines issued by DPSS from time to time.
4. Banks are advised to block a lost card immediately on being informed by the customer and formalities, if any, including lodging of FIR can follow within a reasonable period.
5. Banks may consider introducing, at the option of the customers, an insurance cover to take care of the liabilities arising out of lost cards. In other words, only those cardholders who are ready to bear the cost of the premium should be provided an appropriate insurance cover in respect of lost cards.

A. *Securing Card Payment Transactions*

Security and Risk Mitigation Measures for Electronic Payment Transactions

Payments effected through alternate payment products/channels are becoming popular among the customers with more and more banks providing such facilities to their customers. While this move of the banks indeed promotes and encourages the usage of electronic payments, it is imperative that the banks ensure that transactions

effected through such channels are safe and secure and not easily amenable to fraudulent usage. One such initiative by RBI, was mandating additional factor of authentication for all card not present (CNP) transactions. Security of card present transactions has also been initiated by RBI through the implementation of recommendations of the Working Group on Securing Card Present transactions. Banks have also put in place mechanisms and validation checks for facilitating on-line funds transfer, such as: (i) enrolling customer for internet/mobile banking; (ii) addition of beneficiary by the customer; (iii) velocity checks on transactions, etc.

With cyber-attacks becoming more unpredictable and electronic payment systems becoming vulnerable to new types of misuse, it is imperative that banks introduce certain minimum checks and balances to minimise the impact of such attacks and to arrest/minimise the damage. Accordingly, banks are required to put in place security and risk control measures as detailed here under:

Securing Card Payment Transactions

i. All new debit and credit cards to be issued only for domestic usage unless international use is specifically sought by the customer. Such cards enabling international usage will have to be essentially EMV Chip and Pin enabled. (By June 30, 2013)

ii. Issuing banks should convert all existing MagStripe cards to EMV Chip card for all customers who have used their cards internationally at least once. (for/through e- commerce/ATM/POS) (By June 30, 2013)

iii. All the active Magstripe international cards issued by banks should have threshold limit for international usage. The threshold should be determined by the banks based on the risk profile of the customer and accepted by the customer (By June 30, 2013). Till such time this process is completed an

omnibus threshold limit (say, not exceeding USD 500) as determined by each bank may be put in place for all debit cards and all credit cards that have not been used for international transactions in the past.

iv. Banks should ensure that the terminals installed at the merchants for capturing card payments (including the double swipe terminals used) should be certified for PCI-DSS (Payment Card Industry- Data Security Standards) and PA-DSS. (Payment Applications -Data Security Standards) (By June 30, 2013)

v. Bank should frame rules based on the transaction pattern of the usage of cards by the customers in coordination with the authorized card payment networks for arresting fraud. This would act as a fraud prevention measure. (By June 30, 2013)

vi. Banks should ensure that all acquiring infrastructure that is currently operational on IP (Internet Protocol) based solutions are mandatorily made to go through PCI-DSS and PA-DSS certification. This should include acquirers, processors / aggregators and large merchants. (By June 30, 2013)

vii. Banks should move towards real time fraud monitoring system at the earliest.

viii. Banks should provide easier methods (like SMS) for the customer to block his card and get a confirmation to that effect after blocking the card.

ix. Banks should move towards a system that facilitates implementation of additional factor of authentication for cards issued in India and used internationally. (transactions acquired by banks located abroad)

x. Banks should build in a system of call referral in co-ordination with the card payment networks based on the rules framed at (v) above.

Chapter-3
REVIEW OF LITERATURE

Review of literature is backbone of every research study. It is important to review the existing literature to have an overview of what kinds of studies have been conducted and what are the gaps in literature. Therefore, various studied in the domain of e-banking which were conducted in India and abroad have been reviewed.

Zeithaml and Gilly (1987) attempted to compare the adoption of retailing technology among elderly and non-elderly bank customers. The study found that main reason for the reason for not using the ATMs was the preference for human tellers.

Marshall and Heslop (1988) in their study attempted to investigate the impact of demographic variable on the adoption of ATM services. The study found that consumers' motives for use of technology were useful for predicting subsequent usage. Demographic factors such as higher education levels and employment status were positively related to usage of ATMs. Age was negatively related to adoption of ATMs.

Leblanc (1990) tried to identify the main consumer motivations for adoption of ATM Study found out that main consumer motivation for using ATMs was its accessibility benefits. Study also found that used of technology in banking sector improved service quality, presented little security risk and fulfilled their need for simple and fast transactions. Furthermore, non-users preferred interacting with human tellers and perceived ATM usage to be complex and risky.

Lewis (1991) found that users mainly used ATMs for withdrawal of cash and obtaining account balances. Study also found that negative factors regarding ATM usage were concern over personal safety, lack of privacy and operational problems

such as machine being regularly out of cash or out of order and cards getting stuck in it.

Rugimbana and Iversen (1994) found that ATM customers mostly used ATM for cash withdrawal and conducted less than 50% of their transactions through it, The study concluded that most users perceived ATMs to be just convenient cash dispensers, while the non-users preferred contact with human tellers and had a need for personal service.

Sathye (1999) examined the factors affecting the adoption of Internet banking by Australian consumers. The sample for this survey was drawn from individual residents and business firms in Australia. Study found that security concerns and lack of awareness about Internet banking and its benefits stand out as being the obstacles to the adoption of Internet banking in Australia.

Polatoglu and Ekin (2001) conducted an exploratory study of consumer acceptance of Internet banking (IB) services in a Turkish bank. Study examined both consumer-related factors that may affect the adoption of an innovation or a product (such as complexity, perceived risk, and relative advantage) as well as organizational factors such as marketing effort. The results suggest that IB not only reduces operational cost to the bank, but also leads to higher levels of customer satisfaction and retention. Accordingly, it is argued that IB is strategically important to the banking sector in an emerging economy, such as in Turkey.

Polatoglu and Ekin (2001) listed nine factors which according to them influenced the diffusion of Internet banking (IB). These factors were ‘relative advantage’, ‘observability’, ‘trialability’, ‘complexity’, ‘perceived risk’, ‘type of group’, ‘type of decision’, and ‘marketing effort’.

Gerrard and Cunningham (2003) identified eight characteristics relating to the adoption of internet banking in Singapore such as 'social desirability', 'compatibility', 'convenience, 'complexity', 'confidentiality', 'accessibility', 'economic benefits' and 'PC proficiency' as eight influential factors of adoption.

Suganthi et al. (2001) conducted the review of Malaysian banking sites and revealed that all domestic banks were having a web presence. Only 4 of the ten major banks had transactional sites. The remaining sites were at informational level. There are various psychological and behavioral issues such as trust, security of Internet transactions, reluctance to change and preference for human interface which appear to impede the growth of Internet banking

Karjaluoto et.al, (2002) explored the effect of different factor in the attitude formation toward internet banking in Finland. For study purpose a sample of 1167 bank customers were taken. Attitude formation was studied with the help of Structural Equation Modeling (SEM). The study found that prior experience & knowledge of computer and attitude toward computer influence attitude toward online banking. The study also found that demographic factors such as occupation and household income impact heavily online banking behavior.

Boon and Yu (2003) attempted to identify the key success factors in the operation of e-channels in the Malaysian banking scenario. For survey purpose self administered questionnaire was distributed among target population of bankers currently employed by locally commercial banks in Malaysia. The findings of the study were based on 112 respondents' opinions. The data was analyzed using simple frequencies and factor analysis. The results of the study showed that bank's operation management is the main factor affecting the success of ATMs and PCs and branch banking. On the other hand product innovation and knowledge innovation factors

were found to have the significant effect on banking kiosks and phone banking respectively. In the end study suggested that domestic commercial banks in Malaysian would have to enhance their operational management in order to succeed in using ATMs and PC Banking as their main e-channels.

Wang et al., (2003) has given the extended version of TAM in the context of acceptance of internet banking. The extended version of TAM included "perceived credibility" as a new factor that reflects the user's security and privacy concerns in the acceptance of Internet banking. Study has also examined the effect of computer self-efficacy on the intention to use Internet banking through perceived ease of use, perceived usefulness and perceived credibility. Based on a sample of 123 users from a telephone interview in Taiwan, the results strongly support the extended TAM in predicting the intention of users to adopt Internet banking. It also demonstrated the significant effect of computer self-efficacy on behavioral intention through perceived ease of use, perceived usefulness, and perceived credibility.

Mattila et al., (2003) in their study analyzed the mature customers' Internet banking behavior in Finland. The survey sample consisted of three consumer segments (non-users, new users, old users) that differed in terms of Internet banking experience and sample size was 1,167 bank customers Household income and education were found to have a significant effect on the adoption of the Internet as a banking channel, so that over 30 percent of wealthy and well-educated mature males make e-banking their primary mode of making payments. Perceived difficulty in using computers combined with the lack of personal service in e-banking was found to be the main barriers of Internet banking adoption among mature customers. Internet banking was also found to be more unsecured among mature customers than bank customers in general.

Geeta (2003) reviewed the current scenario of phishing attacks in India and provided some countermeasures that can be adopted by online firms to fight this kind of attack. The study found that there has been an increase in identity theft in the last few years which could pose a serious problem in the future, resulting in loss of trust by the customer towards net banking. Most of the Indian banks are taking initiatives to address the problem but still more work is to be done in the case of small and rural banks. In the end, the study furnished guidelines to tackle the situation.

Hutchinson and Warren (2003) proposed a framework concerning how to identify security requirements for internet banking so that the transaction being conducted are secured within their respective environments.

Wan et al., (2004) in their study investigated factors that influenced Hong Kong bank customers' adoption of four major banking channels, i.e. branch banking, ATM, telephone banking, and internet banking. Specifically, the study aimed to focus on the influences of demographic variables and psychological beliefs about the positive attribute possessed by the channels. Based on survey of 314 bank customers, study found that ATM was the most frequently adopted channel, followed by internet banking and branch banking, and telephone banking was the least frequently adopted channel. Psychological beliefs about the extent to which a channel possessed certain positive attributes were more predictive of adoptions of ATM and internet banking than adoptions of branch banking and telephone banking. Further, demographic backgrounds were strongly associated with adoption of all banking channels except ATM.

Shih and Fang (2004) attempted to understand the influence of individual's belief, embracing attitude, subjective norm and perceived behavioral control on intention. Two versions of the model of the theory of planned behavior (TPB) – pure

and decomposed were examined and compared to the theory of reasoned action (TRA). Data were collected from approximately 425 respondents and structural equation modeling was used to analyze the responses. Results supported TRA and TPB and provide a good fit to the data.

Pikkarainen et al., (2004) found that' perceived usefulness' and 'ease of use' were the main factors influencing the internet banking acceptance.

Jaruwachirathanakul and Fink (2005) attempted to identify the factors that encourage consumers to adopt internet banking services in Thailand. The study was based on the Decomposed Planned Behaviour. For the purpose of data collection a sample of 506 people was taken from 40 large companies in Bangkok. The study found that attitudinal factors that appeared to encourage the adoption of internet banking in Thailand most were "Features of the web site" and "Perceived usefulness", Further, most significant obstacle to adoption was a perceived behavioural control, namely "External environment". The significant moderating factors were gender, educational level, income, internet experience and internet banking experience, but not age. In the end study suggested that, it is essential for banks to facilitate encouragement and restrict impediment factors. Therefore, in addition to the direct "push" from internet banks (in respect of the encouragement factors), indirect persuasion should be carried out as a "pull" mechanism (in respect of the impediment factors).

Bauer et al., (2005) validated a measurement model for the construct of web portal quality based on the dimensions: security and trust, basic services quality, cross-buying services quality, added value, transaction support and responsiveness. The study identified dimensions could reasonably be classified into three service categories: core services, additional services, and problem-solving services.

Ndubisi and Sinti (2006) examined the determinant structure of customers 'attitude and system's characteristics on adoption of internet banking (IB) by Malaysian bank customers. The research framework links attitudinal constructs such as importance of IB to customers' banking needs, compatibility, complexity, trialability, and risk to internet banking adoption. Moreover, the impact of IB site design characteristics on adoption was also verified. An online questionnaire was used in this research and respondents were approached through extensive personalized email invitations as well as postings to the newsgroups. The results of the study reveal that the attitudinal factors play a significant role in internet banking adoption. Moreover, utilitarian orientation of the website rather than hedonic orientation has significant influence on adoption.

Flavian and Guinalu (2006) analyzed how consumers' perceptions about their traditional bank influence their decision to adopt the services offered by the same bank on the internet. The primary data was collected by using survey from customers of various banks totaling 633, which distribute their services by traditional channels as well as on the internet. A Binomial Logistic Regression process was analyzed to assess the influence of trust, incomes, age, sex, education and employment on the adoption of the financial services offered by a traditional bank on the internet. The study showed that consumer trust in a traditional bank, as well as incomes, age and sex were factors that influence consumers' decision to work with the same bank via the internet.

Gerrard et al., (2006) attempted to find out factor which were responsible for not using internet banking. For study purpose, a survey was used to acquire data from 127 consumers who were not internet user. Using a content analysis procedure, eight factors were identified which explain why consumers were not using internet banking.

the identified factors were perceptions about risk; the need; lacking knowledge; inertia; inaccessibility; human touch; pricing and IT fatigue.

Malhotra and Singh (2007) attempted to discover the factors affecting a bank's decision to adopt Internet banking in India. The study has examined the relationship between the bank's adoption decision and various bank and market characteristics. The data for the study consisted of panel data of 88 banks in India covering the financial years 1997-1998 to 2004-2005. To establish the relationship Logistic regression technique was employed. The results showed that the larger banks, banks with younger age, private ownership, higher expenses for fixed assets, higher deposits and lower branch intensity evidenced a higher probability of adoption of internet banking. Study further found that banks with lower market share also saw the Internet banking technology as a means to increase the market share by attracting more and more customers through this new channel of delivery.

Alam et al., (2007) examined the development and prospects of internet banking in Bangladesh. Study found that lack of infrastructure was the major issues for internet banking. As per author's opinion, Bangladesh banks were reluctant to use full internet base banking activities. Nationalized commercial banks were far behind implementing internet banking system in banking transactions when compared with private and foreign banks. Nationalized commercial banks provide ATM services with very few branches and also the computerized branches were very small except the foreign commercial banking.

Sayar and Simon (2007) compared and evaluated the internet banking services of Turkey and the UK. For study purpose a sample of nine banks from each country taken and a web survey was conducted to collect data for each internet bank using an analytical framework based on a three dimensional model. Study found that Turkish

banks offered a wider range of services from their internet branches compared to British banks, despite the fact that the UK had a more favourable environment for internet banking in terms of the level of sophistication of its banking sector and technological infrastructure. Study further observed key difference in the approaches of banks towards the issue of 'security' where Turkish banks rely on technology to avoid fraud and British banks prefer more conventional methods to discourage it.

Abu and Pearson (2007) investigated the key determinants of the adoption of internet banking in Jordan. The study also attempted to validate the appropriateness of the Unified Theory of Acceptance and Use of Technology (UTAUT) within the context of internet banking. The results of the study indicated that UTAUT provided a good foundation for future technology acceptance research. The three main predictors relevant to this study (performance expectancy, effort expectancy, and social influence) were significant and explained a significant amount of the variance in predicting a customer's intention to adopt internet banking. The results also indicated that gender moderated the relationships.

Laukkanen (2007) compared customer perceived value and value creation between internet and mobile bill paying service. A qualitative in-depth interviewing design was applied in order to ascertain the factors that create value perceptions in fund transfer service via personal computer and mobile phone. The results indicated that customer value perceptions in banking actions differed between internet and mobile channels. The findings suggested that efficiency, convenience and safety are salient in determining the differences in customer value perceptions between internet and mobile banking.

Celik, Hakan (2008) in his study provided an insight into the determinants of customers' acceptance to internet banking. The study has addressed a research need

for extending the technology acceptance model (TAM) by adding contextual factors for the case of Internet banking. The additional contextual factors added to model were perceived behavioral control (PBC), perceived playfulness (PPL) and perceived risk (PR). The partial least squares (PLS) procedure is used to analyze 161 cases collected from individual Internet banking users through a web-based survey. The results indicated that perceived usefulness (PU) and perceived ease of use (PEOU) are immediate direct determinants of customers' attitudes towards using Internet banking. PU, PR and ATT determine the large proportion of behavioral intentions to use Internet banking. Although PPL positively influences only PEOU, PBC exerts positive direct effects on PEOU and PU and indirect effects on PU and ATT. Study also found that Perceived Risk i.e. concern for security and privacy could be one of the obstacles for IB adoption and its adverse effects should not be underestimated by practitioners.

Poon (2008) explored the determinants of users' adoption momentum of e-banking in Malaysia. For study purpose sample to 324 bank customers was taken. In the present study, ten attributes were tested, namely convenience of usage, accessibility, features availability, bank management and image, security, privacy, design, content, speed, and fees and charges. Results indicated that all elements for ten identified factors were significant with respect to the users' adoption of e- banking services. Privacy and security were the major sources of dissatisfaction, which have momentously impacted users' satisfaction. Meanwhile, accessibility, convenience, design and content were sources of satisfaction. Besides, the speed, product features availability, and reasonable service fees and charges, as well as the bank's operations management factor were critical to the success of the e-banks. WAP, GPRS and 3G features from mobile devices had no significance or influence in the adoption of e-

banking services. Results also revealed that privacy, security and convenience factors play an important role in determining the users' acceptance of e-banking services with respect to different segmentation of age group, education level and income level.

Amin (2008) investigated the factors that affecting the adoption of new mobile phone credit card technology by bank customers in Malaysia. The study extended the applicability of the technology acceptance model (TAM) to mobile phone credit cards and includes 'perceived credibility (PC)', the 'amount of information about mobile phone credit cards (AIMCs)' and 'perceived expressiveness (PE)', in addition to 'perceived usefulness (PU)'' and 'perceived ease of use (PEOU)'. The study indicated that PU, PEOU, PC and the amount of information contained on mobile phone credit cards were important determinants to predicting the intentions of Malaysian customers to use mobile phone credit cards. However, PE was not an important determinant in predicting the intentions of Malaysian customers to use mobile phone credit cards.

Krauter and Faullanta (2008) investigated the role of internet trust as a specific form of technology trust in the context of internet banking. Study further investigated the integration of propensity to trust within the hierarchical structure of personality and its applicability to technological systems. The results confirmed the influence of internet trust on risk perception and consumer attitudes towards internet banking. It was also found that propensity to trust was a determinant not only for interpersonal relationships but also for trust in technological systems

Ho and Ku (2008) investigated the impact of self-service technology (SST) to enhance customer value (CV) and customer readiness (CR). Study also inspected the effects of CV and CR in customers' continued use of Internet banking. Study found that SST characteristics (i.e. ease of use, usefulness, costs saved, and self-control)

demonstrated positive effects on CV and CR. CR was positively related to CV. Furthermore, customers expressed their willing to use Internet banking when CV and CR are high.

Laukkanen et al., (2008) attempted to understand the innovation resistance by dividing internet banking non-adopters into three groups i.e., postponers, opponents and rejectors. Study also aimed to identify how the resistance differs in customer groups. The data were collected by conducting a postal survey among the retail banking customers in Finland who had not adopted internet banking. The study found significant differences between the groups explored. The resistance of the rejectors was much more intense and diverse than that of the opponents, while the postponers showed only slight resistance. The results also indicated that psychological barriers were even higher determinants of resistance than usage and value, which were constructs related to ease-of-use and usefulness determining acceptance in the traditional technology acceptance model. Moreover, the findings highlighted the role of self-efficacy in bank customers' risk perceptions to internet banking.

Polasik and Wisniewski (2009) in their study attempted to identify the factors underlying the decision to adopt online banking in Poland. The research was based on the conceptual model where factors which were hypothesized to influence the individual's decision to adopt internet banking were categories into six main categories: perceived security; internet experience; marketing exposure; use of other banking products; type of internet connection used; and demographic characteristics. Three of these categories (internet experience, Use of other banking products and Demographic characteristics) were divided into more detailed sub-groups. The sample used in this study was 3,519 Polish internet users. The dichotomous decision of whether to adopt internet banking services was assessed, via Binomial Logistic

Regression, to numerous explanatory variables. The study found that a dominant relationship has been observed between the decision to open an online account and the perceived level of security of internet transactions. Experience with the medium of internet and certain demographic variables also proved to be robust predictors of the adoption status. Moreover, advertising appeared to be efficacious and that online banking interacts with consumption of other products offered by banks. In the end study suggested that financial institutions can encourage customers to use this cost-effective distribution channel through carefully-planned actions.

Rod et al., (2009) examined the relationships among three dimensions of service quality that influence overall internet banking service quality and its subsequent effect on customer satisfaction in a New Zealand banking context. The results showed significant relationships among online customer service quality, online information system quality, banking service product quality, overall internet banking service quality and customer satisfaction.

Chong et al., (2010) attempted to empirically examine the factors that affect the adoption of online banking in Vietnam. In the study, perceived usefulness, perceived ease of use, trust and government support were examined to determine if these factors were affecting online banking adoption. Based on opinion of 103 bank customers, study found that perceived usefulness, trust and government support all positively associated with the intention to use online banking in Vietnam. The study further showed that trust in security and privacy of online banking would influence the adoption of online banking in Vietnam. Without proper security and privacy protection, users would not use the online banking services provided by the banks. Contrary to the technology acceptance model, perceived ease of use was found to be not significant.

Tommi and Vesa (2010) investigated the effect of information and guidance offered by a bank on five adoption barriers; usage, value, risk, tradition and image in a mobile banking context. A survey was conducted on 1551 bank customers in Finland. The results showed that the information and guidance offered by a bank had the most significant effect on decreasing the usage barrier, followed by image, value and risk barriers respectively. The information and guidance showed no effect on the tradition barrier.

Wessels and Drennan (2010) aimed to identify and test the key motivators and inhibitors for consumer acceptance of mobile phone banking (M-banking), particularly those that affect the consumer's attitude towards, and intention to use, this self-service banking technology. A web-based survey was undertaken where respondents completed a questionnaire about their perceptions of M-banking's ease of use, usefulness, cost, risk, compatibility with their lifestyle, and their need for interaction with personnel. Based on results, perceived usefulness, perceived risk, cost and compatibility were found to affect consumer acceptance of M-banking. The results also supported a mediation model, whereby attitude transfers the affects of the consumers' perceptions to their intention to use M-banking.

Zhao and Lewis (2010) in their study examined the roles of trust and perceived risk on consumers' internet banking services (IBS) usage intention. For study purpose, an integrated model explaining the interrelationships between trust, perceived risk and usage intention was developed. The research was conducted on a sample of 432 young Chinese consumers who can be classified as early adopters of internet banking. Results indicated that there was a significant relationship between trust and perceived risk and that both were crucial in explaining the internet banking usage intention. Furthermore, trust in the bank is fundamental not only to reducing

risk perceptions of IBS in general but also to building trust in the banks' competence in terms of IBS activity.

Nor and Mastor (2010) examined the influence of perceived ease of use, perceived usefulness, and trust on the intention to use internet banking among Malay and Chinese ethnic groups. The target group for study was final year business students and Master of Business Administration students at four public universities in Malaysia. Study found that, for both ethnic groups, perceived usefulness, perceived ease of use and trust had significant effect on the intention to use internet banking. Further, regression coefficients revealed the cultural traits that may explain the extent to which they influence factors that affect the intention to use.

Yap et al., (2010) examined the role of situation normality cues (online attributes of the e-banking web site) and structural assurance cues (size and reputation of the bank, and quality of traditional service at the branch) in a consumer's evaluation of the trustworthiness of e-banking and subsequent adoption behavior. Study found that traditional service quality builds customer trust in the e-banking service. The size and reputation of the bank were found to provide structural assurance to the customer but not in the absence of traditional service quality. Web site features that give customers confidence were significant situation normality cues.

Malhotra and Singh (2010) presented the status of Internet banking in India and the extent of Internet banking services offered by Internet banks. It also examined the factors affecting the extent of Internet banking services. Study found that the private and foreign Internet banks had performed well in offering a wider range and more advanced services of Internet banking in comparison with public sector banks. Among the determinants affecting the extent of Internet banking services, size of the

bank, experience of the bank in offering Internet banking, financing pattern and ownership of the bank were found to be significant

Ho and Lin (2010) developed a multiple item scale for measuring internet banking service quality. This research adopted the dimensions of electronic service quality (e-service quality) and customer-perceived service quality to develop a framework that could be used to measure internet banking service. This research used Taiwan's internet banking users as sample. After applying the factor analysis five dimensions and 17 items in the measurement scale for measuring the service quality of internet banking were identified. The five dimensions were named customer service, web design, assurance, preferential treatment, and information provision

Safeena et al., (2010) conducted a study on adoption of internet banking and found that 'Perceived usefulness', 'Perceived ease of use' and Perceived risks are the important determinants of online banking adoption

Salhieh, et al., (2011) conducted a study to propose and validate a framework that can be used for assessing the level of banks' readiness for providing e-banking services in Jordan. The population of the study included 18 commercial and Islamic banks in Jordan. The sample consisted of 60 managers, 30 IT mangers and 150 customers. The study used three constructs to propose a framework that can assess e-banking readiness: perceptions of bankers, perceptions of customers, and IT infrastructure in banks. Study found that e-banking had achieved a degree of strategic and operational importance among bank managers. Also, customers are positive about embracing new banking channels. But it seemed that technological aspects and IT employees' skills were paramount concerns.

Zhou (2011) examined the effect of initial trust on mobile banking use adoption in china. The results indicated that structural assurance and information

quality were the main factors affecting initial trust, whereas information quality and system quality significantly affected perceived usefulness. Initial trust affected perceived usefulness, and both factors predicted the usage intention of mobile banking

Mei Xue et al., (2011) that customers who have greater transaction demand and higher efficiency, and reside in areas with a greater density of online banking adopters, are faster to adopt online banking after controlling for time, regional, and individual characteristics

Kesharwani and Bisht (2012) attempted to test the extended version of TAM (Technology Acceptance Model) in the context of internet banking adoption in India under security and privacy threat. Researchers have conceptualized the model by incorporating various inhibitors of internet banking which restrict the use of internet banking adoption under "perceived risk". They also considered the role of the bank website as a key determinant of perceived risk and of perceived ease of use in the context of internet banking services. For data collection, a sample of 740 students of a business school was selected. Study found that that perceived risk had a negative impact on behavioral intention of internet banking adoption and trust has a negative impact on perceived risk. A well-designed web site was also found to be helpful in facilitating easier use and also minimizing perceived risk concerns regarding internet banking usage. In the end, study suggested that financial bank institutions should give attention to the inhibitors or perceived risk factors of internet banking adoption in order to retain existing customers as well as attract new consumers. The study also suggests that banks should build a web site with features to facilitate users' assessment of internet banking services and thus minimize the perceived risk and maximize the perceived ease of internet banking services. Web-based retailers

depending on online payments would also be benefit by incorporating the elements of perceived risk and trust in their own web design and online services.

Yousafzai and Soriano (2012) examined customers' actual internet banking behaviour by combining the construct of technology readiness with the technology acceptance model and demographics, such as age and gender, into one integrated framework. The tested model was named as 'The customer-specific internet banking acceptance model (CSIBAM)'. For study purpose a sample of 435 UK internet banking users was taken. The results indicated that technology readiness, age and gender moderate the beliefs-intention relationship. Customers with varying levels of technology-related views and demographics hold different beliefs about technology. The relationship between usefulness and behaviour was stronger for younger males with high levels of optimism and innovativeness (explorers and pioneers), whilst the relationship between ease of use and behaviour was stronger for older females with a high level of discomfort (paranoids and laggards).

Moscato and Altschuller (2012) highlighted the significance of user perceptions of security by examining the content of the security policies of banks throughout the world. The security policy was illustrated as a tool for banks to use to manage their users' perceptions. The investigation also uncovered some notable differences among the expected security concerns within different regions. Study found that cumulative percentage of security features mentioned, the United States, the Americas, and Europe/Australia range from 352-384% whereas in China, Japan, and Africa these features were only cumulatively 221% Study suggested that banks understand their target audiences' e-commerce backgrounds, they can more effectively manage their potential users' perceptions of security

Kesharwani and Bisht (2012) attempted to extend the technology acceptance model (TAM) in the context of internet banking adoption in India under security and privacy threat. The study revealed that perceived risk had a negative impact on behavioral intention of internet banking adoption and trust had a negative impact on perceived risk. A well-designed web site was also found to be helpful in facilitating easier use and also minimizing perceived risk concerns regarding internet banking usage.

Zhu and Chen (2012) explored and empirically tested fairness in predicting online customer satisfaction in the internet banking context. The paper also explored the mechanism through which fairness influences customer satisfaction online, i.e. identifying the mediators. The study found that in internet banking, fairness that includes distributive fairness, procedural fairness and informational fairness was positively related to customer satisfaction. Further, trust was identified as the key mediator of fairness to customer satisfaction

Giovanis et al., (2012) proposed and tested an extended technology acceptance model (TAM) with the purpose to examine the factors affecting Greek customers' intentions to adopt internet banking services. Further, several individual differences were examined, with respect to their impact on the formation of customers' attitude about the pros and cons of the new technology. The study validated a causal model linking the constructs of the proposed service's compatibility, perceived ease of use, perceived usefulness, perceived security and privacy risk, customers' demographics and IT competences, with customers' intentions to adopt internet banking services in the future, by collecting data from off-line banking customers that were familiar with the internet The results indicated that service compatibility is the key factor, which mostly shapes customers' behavioural intentions toward internet banking adoption,

followed by TAM constructs and perceived risk elements. Moreover, TAM and perceived security and privacy risk constructs partially mediate the relationships between compatibility and customers' behavioural intentions, while perceived usefulness partially mediates the relationship between perceived ease of use and customers' intentions. Finally, in terms of the impact of individual differences on customers' beliefs about internet banking compatibility, value and risk elements, younger, mostly male customers, with adequate previous IT experience who find themselves to be compatible with the new service, are a more promising target group to use internet banking, as an alternative channel to perform their financial transactions in the future.

Patsiotis (2012) examined internet banking adoption and resistance behaviour in Greece in order to develop profiles of adopters and non-adopters of the service. The study identified three segments, where the description of their profiles was based on customer perceptions of the service and general usage data. Across these segments adopters and non-adopters were found to have different characteristics. With regard to demographics, only income was found to be associated with segment membership

Akturan and Tezcan (2012) investigated consumers' mobile banking adoption through an integration of the technology acceptance model (TAM) with work on perceived benefits and perceived risks. Data were collected from 435 university students who were non-users but future prospects, and analyzed by structural equation modeling (SEM). It was found that perceived usefulness, perceived social risk, perceived performance risk and perceived benefit directly affect attitudes towards mobile banking, and that attitude is the major determinant of mobile banking adoption intention. In addition, no direct relationship between perceived usefulness and intention to use, perceived ease of use and attitude, financial risk, time risk, security/ privacy risk and attitude was detected.

Singh and Kaur (2012) compared the pre-login and after login features of two banks' online portals in India. A content analysis technique was used to study the listed features of selected websites. Study found that selected banks' online portals differ on various features such as accounts information, fund transfer, online requests and general information. In the end, study suggested to include the good feature of other online portal which would help them to make their sites more secure, informative and user friendly.

Subsorn and Limwiriyakul (2012) investigated that there was a distinct lack of internet banking security information provided on all the selected Thai banks' websites as compared to the selected Australian banks which provided better internet banking security information.

Thakur and Srivastava (2013) investigated the factors influencing the adoption intention of mobile commerce. For the study purpose research model was developed based on constructs from the technology acceptance model and innovation resistance theory. Perceived usefulness, perceived ease of use and social influence were found to be significant dimensions of technology adoption readiness to use mobile commerce while facilitating conditions were not found to be significant. The results also indicated perceived credibility risk defined by security risk and privacy risk was significantly associated with behavioural intention in negative relation, which indicated that security and privacy concerns are important in deterring customers from using mobile commerce.

Mzoughi and Sallem (2013) described three profile segments (postponers, opponents and rejectors) of non-adopters of internet banking in Tunisia, and attempted to predict consumers' willingness to adopt this new technology using a range of factors. Significant differences were observed between the three segments (postponers, opponents and rejectors) on the basis of the proposed predictors.

Moreover, dispositional resistance to change as a personality trait played a significant role in behavioral intentions.

Maditinos et al., (2013) developed an extended technology acceptance model (TAM) model as a tool for examining the factors that have a significant impact on customers' online banking acceptance. The typical TAM constructs were enhanced with the variables of perceived risk and quality of the internet connection. The proposed conceptual framework of the study (extended TAM), was tested on a sample of Greek internet users. The findings of the study provided overall support for the extended TAM model and confirmed its robustness in predicting customers' intention of adoption of internet banking. More specifically, results underlined the important impact of perceived usefulness, security risk and performance risk on the intention to use internet banking. On the contrary, the impact of perceived ease of use and quality of the internet connection seemed to have only an indirect effect on internet banking adoption.

Narteh (2013) identified the dimensions of Automated Teller Machine (ATM) service quality and to evaluate customers' perceptions of the relative importance of these dimensions in Ghana. The paper identified five dimensions of the "ATMqual" model. In order of importance, these dimensions were reliability, convenience, responsiveness, ease of use and fulfillment. Study suggested that delivery of financial services over the Internet should be a part of overall customer service and distribution strategy. These measures could help in rapid migration of customers to Internet banking, resulting in considerable savings in operating costs for banks.

Gaps in Review of Literature

Review of literature reveals that e-banking services such as Internet Banking, ATMS, Mobile banking, Phone Banking, Cards have received significant amount of

interest from academicians especially in the recent times. Majority of studies have been conducted on identification factors influencing the adoption of e-banking services, application of extended Technology Acceptance Model (TAM) to e-banking sector, behavior of non users of e-banking services, impact of demographic of adoption of e-banking services, development scale to measure e-service quality, understanding resistance to e-banking services behavior etc. It is observed that perceived risk, trust security and privacy reminded the integral part of majority of the studies. However, only few studied have been conducted to address the security and privacy issues. Moreover, these studies primarily focused on prevailing security and privacy practices of banks regarding e-banking channel rather than customers' perceptions. Further, in India there is dearth of literature on e-banking services only few studies are available in this regard. From the available sources, research could not find even a single study which has been conducted in India to understand the perception of bank customers; perception toward 'security and privacy concern' and 'security and privacy satisfaction' regarding use of e-banking services. Thus, gaps have been found in available literature and present study attempts to fill these gaps.

Chapter – 4
RESEARCH METHODOLOGY

The present study examines the security and privacy issues in e-banking. With a view to develop a sound theoretical framework for investigation, review of literature in related to e-banking services and security issues has been carried out in the previous chapter. Important studies related to adoption of e-banking services, security issues in e-banking services etc. conducted in India as well abroad have been reviewed.

The present study has three dimensions. Firstly it studies the security features of online banking portals where online banking portals of selected banks have been compared on the basis of security and privacy features. Secondly, it examines the perception of bank customers towards security and privacy issues in e-banking. Thirdly, it attempts to understand the view of non users of e-banking services. Therefore, it is important to know how these three dimensions have been studied. Hence, the present chapter discusses the research methodology that has been used in the present study.

4.1 Research Design

A *research design* is the overall plan for obtaining answers to the questions being studied and for handling some of the difficulties encountered during the research process. Hair et al. (2000: 37) believe that most research objectives can be met by using one of three types of research design: exploratory, descriptive or causal. In present research study, an exploratory-cum-descriptive research design has been used.

4.2 Scope of the study

Every research has to be limited in its theoretical and geographical scope. A limited scope is helpful in intensive study of the research problem. The theoretical scope of the study is limited to e-banking services of four banks i.e. ATM, Internet Banking, Mobile Banking and Credit cards. The geographical scope of the study was Tri-city i.e. Chandigarh UT, Mohali and Panchkula. Judgment and convenience guided the choice of geographic scope.

4.3 Population, Sampling and Sample Size

The population for the study comprised of customers of selected public and new private sector banks in the tri-city i.e. Chandigarh, Panchkula and Mohali. For study purpose, four banks, two each from public and private sector were selected. More specifically, the target population for the study was defined as "Bank customers who have used at least one e-banking service two times in the last quarter".

The selected banks were top most banks in each sector based on Alexa ranking of websites. The selected banks for the study were State Bank of India (SBI), Punjab National Bank (PNB), ICICI Bank (ICICI), and HDFC Bank (HDFC).

The prime objective of the study was to examine the perception of bank customers regarding security and privacy concern in selected banks. Therefore a sample of 200 bank customers divided equally among selected banks was planned. However, the researcher could obtain only 190 valid questionnaires. Thus, the findings of this study are based on opinion of 190 respondents.

The sampling technique used in the study was Non-Probability Judgmental Sampling[13]. The prime reason for using Judgmental Sampling was the non availability

[13] Judgmental sampling is a form of convenience sampling in which the population elements are selected based on the judgment of the researcher.(Malhotra 2010)

of Random Sampling Frame. Further, opinion of 20 bank customers about not using a particular e-banking service has been analyzed.

4.4 Sampling Unit: Sampling unit for data collection was individual bank customers

4.5 Instruments Design

Two instruments were prepared for data collection purpose i.e. Check List and Questionnaire. A Check List (Annexure-I) was prepared for the purpose of comparing the security and privacy contents of selected online bank portals. It was prepared after perusing the selected online portals. Further, advice of internet security experts and help from previous studies was taken into account. The check list so prepared primarily focused on security and privacy contents of online portals such as general online security and privacy information to the internet banking customers, Information technology assistance, bank site authentication technology and user site authentication technology.

To collect the data from bank customers, a structured questionnaire (Annexure-II) was prepared. The questionnaire was prepared in consultation with banking experts especially in the field of e-banking. Researcher also took into account the inputs of e-banking users to include important aspects of e-banking security in the questionnaire. The first part of the questionnaire dealt with the demographic profile of the respondents. The second part of the questionnaire consisted of eight constructs which were used to measure the level of security & privacy concern and level of satisfaction regarding security & privacy concerns of e-banking services. Respondents were asked to indicate their opinion on Five-Point Likert Scale ranging from ‘strongly agree’ to ‘strongly disagree’ The description of each construct has been shown in Table 4.1.

Table 4.1
Construct used in the study

Sr. No.	Name of Construct	Purpose	No of Items	Author
1	Security and Privacy Concern : ATM	To measure level of Security and Privacy Concern regarding use of ATM	9	Self Constructed
2	Security and Privacy satisfaction :ATM	To measure level of Security and Privacy satisfaction regarding use of ATM	10	Self Constructed
3	Security and Privacy Concern :Internet Banking	To measure level of Security and Privacy Concern regarding use of Internet Banking	8	Self Constructed
4	Security and Privacy satisfaction :Internet Banking	To measure level of Security and Privacy satisfaction regarding use of Internet Banking	11	Self Constructed
5	Security and Privacy Concern :Mobile Banking	To measure level of Security and Privacy Concern regarding use of Mobile Banking	10	Self Constructed
6	Security and Privacy satisfaction :Mobile Banking	To measure level of Security and Privacy satisfaction Regarding use of Mobile Banking	10	Self Constructed
7	Security and Privacy Concern :Credit card	To measure level of Security and Privacy Concern Regarding use of Credit Card	5	Self Constructed
8	Security and Privacy satisfaction :Credit Card	To measure level of Security and Privacy satisfaction Regarding Credit Card	8	Self Constructed

4.6 Reliability and Validity of the Instruments

Both the instruments were checked for reliability and validity. The first instrument i.e. 'Check List' required content validity only. The content validity of the 'Check List' was done by three experts, one from banking field and two academicians.

The second instrument i.e. questionnaire was checked for Reliability and Validity. The reliability of each construct was checked using Cronbach's Alpha[14]. Nunnaly (1978) has indicated 0.7 to be an acceptable reliability coefficient but lower thresholds are sometimes used in the literature. Results of reliability test are based on final survey and are shown in following Tables.

[14] Cronbach's α (alpha) is a coefficient of internal consistency. Alpha coefficient ranges in value from 0 to 1 and may be used to describe the reliability of factors extracted from dichotomous (that is, questions with two possible answers) and/or multi-point formatted questionnaires or scales (i.e., rating scale: 1 = poor, 5 = excellent). The higher the score, the more reliable the generated scale is.

Table 4.2
Reliability of construct Security and Privacy Concern: ATM

Item code	Item description	Item-Total Correlation	Alpha if Item Deleted	Cronbach's Alpha
ATMC1	My ATM PIN may be stolen	.562	.815	.834
ATMC2	My ATM card may be cloned (duplicated)	.548	.817	
ATMC3	My ATM may dispense less amount of currency than requested by me	.584	.813	
ATMC4	Someone may withdraw cash from my ATM without using my card	.638	.807	
ATMC5	Someone can transfer cash from my ATM without using my card	.561	.816	
ATMC6	There may be deduction in my balance without any transaction	.447	.827	
ATMC7	My card information may be shared by the bank with Third party	.519	.820	
ATMC8	Others may see my password while entering it	.562	.815	
ATMC9	I will not get my card back if stuck in ATM	.466	.826	

Table 4.2 shows that Cronbach's Alpha is .834 (>.7, Nunnaly, 1978), the Item-Total Correlation for all items is more than 0.2 (Field, 2005) and none of item resulted in higher than .834 alpha, if deleted. Thus, construct was found to be reliable.

Table 4.3
Reliability of construct Security and Privacy Satisfaction: ATM

Item code	Item description	Item-Total Correlation	Alpha if Item Deleted	Cronbach's Alpha
ATMS1	It is safe to withdraw the cash from my banks' ATMs	.212	.623	.710
ATMS2	My PIN can't be hacked while using my banks' ATMs	.242	.616	
ATMS3	It is not possible for others to see my password while entering	.307	.603	
ATMS4	My ATM card can't be cloned (Duplicated)	.306	.602	
ATMS5	My Bank guides me about security tips from time to time	.274	.632	
ATMS6	There is limit of maximum number of incorrect password submissions	.262	.629	
ATMS7	Contact information is easily available to block my ATM card	.288	.627	
ATMS8	Door of the ATM Cabin has secure access	.399	.578	
ATMS9	There is adequate privacy while using ATM	.546	.540	
ATMS10	Only one person is allowed to enter ATM Cabin for transaction.	.417	.573	

Table 4.3 shows that Cronbach's Alpha is .710 (>.7, Nunnaly, 1978), the Item-Total Correlation for all items is more that 0.2 (Field, 2005) and none of item results in higher than .710 alpha, if deleted. Hence, construct was found to be reliable.

Table 4.4
Reliability of construct Security and Privacy Concern: Internet Banking

Item code	Item description	Item-Total Correlation	Alpha if Item Deleted	Cronbach's Alpha
IBC1	My internet banking password may be stolen	.516	.809	.825
IBC2	Funds may be fraudulently transferred from my account to other's account	.585	.799	
IBC3	I may provide internet banking password at fake websites by mistake	.487	.814	
IBC4	One can monitor my financial transaction history	.591	.798	
IBC5	Bank will not refund my money back if there is online fraud	.416	.821	
IBC6	My account related may be shared by the bank with third party	.583	.800	
IBC7	My online behaviour may be shared with third party	.604	.796	
IBC8	Internet banking is vulnerable to fraud	.610	.798	

Table 4.4 shows that Cronbach's Alpha is .825 (>.7,Nunnaly, 1978), the Item-Total Correlation for all items is more that 0.2 (Field, 2005) and none of item results in higher than .825 alpha, if deleted. Thus, construct was reliable.

Table 4.5
Reliability of construct Security and Privacy Satisfaction: Internet Banking

Item code	Item description	Item-Total Correlation	Alpha if Item Deleted	Cronbach's Alpha
IBS1	It is safe to use internet banking of my bank	.553	.830	.844
IBS2	The site has virtual keyboard to enter Password and User ID	.590	.825	
IBS3	The site provides security guidelines on home page	.604	.828	
IBS4	OTP(One Time Password) is required, if logging from different browsers/computers	.641	.821	
IBS5	OTP is required while making Third Party payments	.505	.832	
IBS6	OTP is always required while adding beneficiary	.561	.828	
IBS7	Pressing back space results in immediately logout from session	.520	.832	
IBS8	Idle time log out from session exists at my Bank's site	.528	.831	
IBS9	There is maximum number of incorrect password submissions	.454	.839	
IBS10	Bank provide me the facility of choosing strong password for internet banking	.588	.826	
IBS11	Bank remind me to change password from time to time	.383	.843	

Table 4.5 shows that Cronbach's Alpha is .844 (>.7, Nunnaly, 1978), the Item-Total Correlation for all items is more that 0.2 (Field, 2005) and none of item results in higher than .844 alpha, if deleted. Thus, construct or the scale was reliable.

Table 4.6
Reliability of construct Security and Privacy Concern: Mobile Banking

Item code	Item description	Item-Total Correlation	Alpha if Item Deleted	Cronbach's Alpha
MBC1	My mobile banking password may be stolen	.659	.834	.856
MBC2	Funds may be fraudulently transferred by using mobile banking	.583	.841	
MBC3	I may provide mobile banking password at fake websites by mistake	.469	.850	
MBC4	Mobile service providers may monitor my financial transaction.	.728	.827	
MBC5	It is very easy for others to 'Add payee' form my mobile banking account	.600	.841	
MBC6	Bank will not refund my money back if there is online fraud	.207	.837	
MBC7	My personal information may be shared by the bank with third party	.693	.830	
MBC8	Mobile banking is vulnerable to fraud	.789	.822	
MBC9	If my phone is stolen, someone else can use my mobile banking	.483	.849	
MBC10	My confidential mobile banking information may be accessed by others through blue tooth	.467	.851	

Table 4.6 shows that Cronbach's Alpha is .856 (>.7, Nunnaly, 1978), the Item-Total Correlation for all items is more that 0.2 (Field, 2005) and none of item results in higher than .856 alpha, if deleted. Thus, construct was found to be reliable.

Table 4.7
Reliability of construct Security and Privacy Satisfaction: Mobile Banking

Item code	Item description	Item-Total Correlation	Alpha if Item Deleted	Cronbach's Alpha
MBS1	It is safe to use mobile banking of my Bank	.481	.658	.721
MBS2	Security guidelines are displayed before using Mobile banking	.213	.713	
MBS3	There is maximum number of incorrect password submissions	.239	.718	
MBS4	My Bank provide me the facility of choosing strong password	.595	.647	
MBS5	OTP (One Time Password) is always required while making Third Party payments	.556	.644	
MBS6	OTP is always required while adding payee account on my site	.400	.669	
MBS7	Pressing back space results in immediately logout from session	.427	.662	
MBS8	Idle time log out from session exists at my Bank's site	.407	.670	
MBS9	My bank does not share my personal information with other sites	.473	.651	
MBS10	My mobile banking site protects information about my onsite behaviour	.306	.687	

Table 4.7 shows that Cronbach's Alpha is .721(>.7, Nunnaly, 1978), the Item-Total Correlation for all items is more that 0.2 (Field, 2005) and none of item results in higher than.721 aplha, if deleted. Thus, construct was reliable.

Table 4.8

Reliability of construct Security and Privacy Concern: Credit card

Item code	Item description	Item-Total Correlation	Alpha if Item Deleted	Cronbach's Alpha
CCC1	My credit card information may be stolen	.695	.754	.817
CCC2	My credit card may be used by others without having my card	.623	.777	
CCC3	I may provide credit card information on fake websites	.542	.801	
CCC4	CVV (password) of my card may be stolen	.608	.783	
CCC5	My card usage information may be shared by bank with others	.577	.791	

Table 4.8 shows that Cronbach's Alpha is .817(>.7, Nunnaly, 1978), the Item-Total Correlation for all items is more that 0.2 (Field, 2005) and none of item results in higher alpha than .817, if deleted. Thus, construct was reliable.

Table 4.9

Reliability of construct Security and Privacy Satisfaction: Credit card

Item code	Item description	Item-Total Correlation	Alpha if Item Deleted	Cronbach's Alpha
CCS1	It is safe to use credit card of my bank	.557	.739	.776
CCS2	Security guideline are always there to use a card	.442	.759	
CCS3	Online usage of card is secure	.524	.744	
CCS4	I always get mobile message for my credit card transaction	.231	.786	
CCS5	CVV of my card can't be hacked	.496	.750	
CCS6	My credit card bill always shows the correct amount spent by me	.365	.769	
CCS7	My credit card information is safe	.681	.717	
CCS8	My bank does not share my card usage information with others	.532	.743	

Table 4.9 shows that Cronbach's Alpha is .776(>.7, Nunnaly, 1978), the Item-Total Correlation for all items is more that 0.2 (Field, 2005) and none of item results in higher than.776 alpha, if deleted. Thus, construct was found to be reliable.

The content validity of all construct was checked by three experts (Two academicians and one banking expert)

4.7 Pre-testing of the Instrument

In order to screen out problems in the instructions or design of a questionnaire, a trial run with a group of 20 bank customers was conducted. The questionnaire was found to have easy understanding and unambiguous statements.

4.8 Data Collection

To collect the data, for the purpose of comparing security and privacy contents of selected online bank portals, researcher registered himself with the selected banks' 'internet banking portals'. The selected online banks' portals were minutely examined and basic internet banking operations was performed for a specific period. Finally, content analysis technique was used to collect the data where the presence or non-presence of security and privacy contents was recorded on the check list for further analysis.

To collect the data from e-banking users, survey method based on the use of self-administered questionnaire was used. Questionnaires were administered to 200 bank customers divided equally among selected banks, however, only 190 questionnaires were found to be valid. At the time of administering the questionnaire an attempt was made to include the respondents from different demographic groups.

Twenty non users of e-banking were also selected in order to find the reasons for not using the e-banking services. These non-users were interviewed by the researchers by asking various open ended questions.

4.9 Period of Survey

The survey of bank customers was carried out during the period of June2013–August 2013.

4.10 Data Analysis

Data collected through survey method was entered in data sheet of SPSS16[15]. The entered data was checked for errors.

4.11 Criterion Measurement of 'security & privacy concern' and 'security & privacy satisfaction'

To measure the level of 'security & privacy concern' and level of 'security and privacy satisfaction' regarding use of e-banking services, 8 self developed Constructs (Table 4.10) were used. Each construct contained set of statements either on 'security & privacy concern' or on security& privacy satisfaction. Mean scores for each statement were calculated by assigning weights of 5, 4, 3, 2 and 1 to 'Strongly Agree', 'Agree', 'Neutral', 'Disagree' and 'Strongly Disagree' respectively. The overall Level of Security and Privacy concern and satisfaction was measured for each construct by calculating the Grand Mean of all the statements' mean for given construct. The mean score for each statement and Grand mean could vary from 1-5. Based on mean scores the level of concern and satisfaction for each construct has been defined as shown in Table 4.10 and 4.11.

Table 4.10

Measuring Level of security and privacy concern regarding use of e-banking services

Mean Scores Range	Level of security and privacy Concern
1-2	Low
2-3	Moderate
3-4	High
4-5	Very High

[15] A statistical Package to analyze the data.

Table 4.11

Measuring Level of Security and privacy satisfaction regarding use of e-banking services

Mean Scores Range	Level of security and privacy Satisfaction
1-2	Low
2-3	Moderate
3-4	High
4-5	Very High

4.12 Statistical Tools

For analysis purpose both descriptive and inferential statistics were used. Descriptive statistics included Percentage, Mean and Standard deviation. Inferential statistics included One-way ANOVA, Kruskal Wallis test and Person's coefficient of correlation.

4.13 Limitations of the study

The study has the following limitations;

1. The time duration to conduct this study was the major constraint. Since obtaining the opinion of customer was not the sole objective of the study, thus sample size was kept limited to 200 (190 Final).
2. Any primary data based study through pre-designed questionnaire suffers from the basic limitation of the possibility of difference between what is recorded and what is the truth , no matter how carefully the interview has been conducted, the questionnaire has been prepared, and field investigation has been done. The same may be true for the present study because the respondents may not deliberately report their true opinion due to their biasness.
3. Some information which might have been useful for the research project was not disclosed by the selected banks due to secrecy and thus the research result are based on available information.
4. The sample used in this study contained a skew toward younger consumers, affecting the generalizability of the results.

Chapter – 5

SECURITY AND PRIVACY ISSUES IN E-BANKING: CONTENT ANALYSIS OF ONLINE PORTALS AND PERCEPTION OF BANK CUSTOMERS

The present chapter has been divided into three sections. The first section compares and discusses the security and privacy features of selected banks's online portals. The second section examines bank customers'perception towards 'security & privacy concern' and 'security and privacy satisfaction' regarding the use of e-banking services. The third section discusses the opinion of non users of e-banking servcies.

Section-I

5. 1 SECURITY AND PRIVACY FEATURES OF ONLINE BANKING PORTALS

To compare the security and privacy features of online banking portal[16], four banks two each from public and private sector were selected on the basis of Alexa Ranking of websites. The selected banks were State Bank of India, Punjab National Bank, HDFC Bank and ICICI Bank. These banks offer internet banking services through their designated online portals i.e. www.onlinesbi.com, www.netpnb.co, www.icicibank.com and www.hdfcbank.com respectively. For the purpose of information collection, researcher registered himself to 'internet banking' service of all the selected banks. After using internet banking for a month, researcher identified various features which seemed to be important from security and privacy perspective. To collect the information about various features of online portals, a content analysis technique was used. Security and privacy features of online portals were analyzed and compared on the basis of 'Pre-Login' and 'Post-Login' features. The Pre-Login and

[16] It is website or web page exclusively dedicated to conduct online banking transactions by internet bank subscribers.

Post-Login information about security and privacy features has been shown in Table 5.1 and Table 5.2 respectively.

5.1.1 Pre-Login Security and Privacy Features

To use the Internet Banking services, a customer has to login to his internet banking account with User Id and password. Bank issues 'User Id' and 'Password' to customer at the time of opening of account either as a part of 'Welcome Kit' or at special request of the customer. Pre-Login features are those features of online portals which a customer comes across at the time of login to his account. There are number of pre-login features of online banking portals. However, keeping in mind the scope of the study, only security and privacy related features have been compared. Bank-wise comparison of Pre-Login features has been shown in Table 5.1.

Table 5.1
Comparison of Pre-Login Features of Online Portal of Selected Banks

Sr. No.	Pre-Login Features	Public Sector Banks		Private Sector Banks	
		SBI	**PNB**	**ICICI**	**HDFC**
i.	Direct access from bank's main home page	**X**	**X**	√	√
ii.	OTP[17] requirement, if logging from different computer or browser	**X**	**X**	√	**X**
iii.	Availability of Virtual Keyboard	√	√	√	√
iv.	Availability of Scrambled Keyboard	√	√	√	√
v.	Availability of Scrambled Keyboard with 'Shuffle' option	**X**	**X**	**X**	√
vi.	Availability of Hovering Keyboard	**X**	**X**	**X**	√
vii.	Multi-Factor Authentication (MFA)	**X**	√	**X**	√
viii.	Alert of leftover attempts in case of wrong passwords	**X**	√	**X**	**X**
ix.	Security Alerts/ Warning message at login page	√	√	√	√
x.	SSL certificate (encryption)	**256bit**	**128bit**	**128bit**	**128bit**

√= ***Feature is Present, X=Feature is not present***

Table 5.1 shows that customers of HDFC Bank and ICICI Bank can login to online banking portal directly from the home page of bank's main website (www.hdfcbank.com and www.icicibank.com) whereas in case of SBI and PNB Bank, no such option is available.

[17] A one-time password (OTP) is a password that is valid for only one login session or transaction.

Customers of SBI and PNB Bank have to login to online banking portals through dedicated domain names i.e. www.onlinesbi.com and www.netpnb.com respectively. In researcher's opinion, it is easy for a customer to login to online banking portal from home page of main website itself. Furthermore, the risk of web spoofing[18] is less, if customers access online banking portal from home page of the bank.

The next security feature of online portals is compulsory entry of 'One Time Password', if a customer login to his internet banking account from different systems or browsers. In this case, if a customer wants to access internet services from different location (systems or browsers), the access to the site will be allowed only after entering OTP which will come on his mobile phone in the form of SMS. This feature makes online portals more secure and prevents unauthorized access. The table shows that this feature is available in case of ICICI Bank only and rest of the banks have not yet introduced it. Thus, first time login to ICICI bank from a different browser or different computers, after entering password, the access will not be granted. Instead, a screen showing one time password with an input able box appears on the screen and access will be granted only after entry of OTP (One Time Password) which comes in the form of SMS on registered mobile.

Another security feature is virtual key of online banking portals. While using virtual key board, a customer has to enter authentication details (User Id and Password) by clicking the on-screen keyboard instead of hard keyboard. Virtual key board secures the websites from key-loggers. All banks' online portals have the option of using virtual keyboard. But its use is optional in nature.

Recently, two more forms of virtual key board have been introduced to provide more security to login process. These forms are 'Scrambled Keyboard' with

[18] Web page spoofing is an activity that hackers use to direct Web site visitors to a Web site that looks like the one they believe they are visiting.

‘Shuffle’ option and ‘Hovering Keyboard’. ‘Scrambled Keyboard’ is an application which is both virtual and dynamic in nature when customer login. In the more advance form, the position of characters on the keyboard changes every time, a character is inserted through the ‘Virtual Keyboard’ if ‘Shuffle’ option is on. On the other hand, ‘Hovering Keyboard’ is a new innovation, which helps customers to enter their banking password by just pointing mouse on the relevant character. This is also called as ‘Mouseover’. Table shows that ‘Scrambled Keyboard’ is available at all selected banks’ online portals. However, advance form of virtual keyboard with ‘Shuffle’ option is available with HDFC bank’ site only. Moreover, ‘Hovering Keyboard’ is present in case of HDFC Bank only.

Multi-Factor Authentication (MFA) strengthens security at login time by using an additional form of ‘authentication’ beyond the standard username and password. The solution is designed to preserve the convenience and usability of online banking while providing additional security for customers. In the process, at the time of entering password, a customer is shown an image and text that have been personalized by him during registration. After analyzing the security features of selected banks’ online portals, it was found that only PNB and HDFC Bank have Multi-Factor Authentication (MFA) system for login. This feature in PNB is known as ‘PNB-IBS Shield' and in HDFC Bank as ‘Secure Access’. SBI and ICICI bank still use standard Authentication process i.e. ‘User Id’ and ‘Password’.

Banks permit up to five attempts for wrong entry of password. More attempts will result in blocking of password. Hence, there must be alert for the customers about leftover attempts which will warn them before entering wrong password. It avoids inconvenience to the customers because of password block. Surprisingly, among selected banks, this feature is available in case of PNB only.

It is general practice that banks alert the user by putting security and privacy messages either on the login page or before the login page. This practice was found in all the selected banks.

SBI has 256-bit Secure Socket Layer whereas rests of the selected banks have 128-bit Secure Socket Layer for encryption[19]. 256-bit Secure Socket Layer for encryption is more secure than 128-bit SSL.

5.1.2 Post-Login Security and Privacy Features

Post-Login feature are those features which customers come across after login to their internet banking account. The comparative picture of post-login features has been highlighted in Table 5.2.

Table 5.2
Comparison of Post-Login features selected banks' online portals

Sr. No.	Post-Login Features	Public Sector Banks		Private Sector Banks	
		SBI	PNB	ICICI	HDFC
i.	Expiry of User ID, if not used	**X**	√	√	**X**
ii.	Expiry of Login Password	**X**	√ **(360d)**	**X**	√
iii.	Expiry of Transaction Password	**X**	√ **(180d)**	**$**	**$**
iv.	Last Login date and Time	√	√	√	√
v.	Mandatory 'Profile Password' to add new payee	√	**$**	**$**	**$**
vi.	OTP to add payee	√	√	**$**	**$**
vii.	Mandatory 'URN' at the time of Online payments	√	√	**X**	**X**
viii.	Assigning Maximum fund transfer limit to an account	√	√	√	√
ix.	Debit Card Grid Authentication to add payee	**$**	**$**	√	√
x.	Mobile alert	√	√	√	√
xi.	Reset Transaction Password online	**X**	√	√	√
xii.	Idle Time log out	√	√	√	√
xiii.	'Backspace'' Fresh' ' Forward' Logout	√	√	√	√

√= Feature is Present, X=Feature is not present $= Not Applicable.

There are clear instructions from PNB and ICICI banks, if user ID is not used for 360 days it will expire. Such instructions prevent unauthorized use of User ID. But this is not the case with HDFC and SBI. Internet banking portals display the last login

[19] Encryption changes plain text into unreadable text using an algorithm.128-bit encryption is so secure that trying to crack it simply isn't feasible.

time and date on web page to alert the internet banking users. User may easily recall time and date of their last visit to the site. If they had not visited the site, it will alert them to take due action. It is found that all selected banks display last login time and date on their portals.

Online security experts always advise that one should change one's password frequently. However, it is general tendency among internet users that they hardly change their passwords. Same is the case with internet banking users. PNB and HDFC have made it compulsory to change the login password after a specified duration. However, ICICI and HDFC banks display password change alert but it is not compulsory to change it. The expiry period of login password and transaction password is 360 days and 180 days respectively in case of PNB. In case of SBI, one needs to enter profile password for number of online transactions. However, this feature is not available in rest of the banks. They use different security methods for this purpose.

The procedure followed by online banking portals to add payee is important security feature. In case of SBI and PNB it is compulsory to enter OTP to Add Payee. But, in case of ICICI and HDFC banks 'Debit Card Grid Authentication' is required. The option to assign maximum transfer limit to account is another security feature. All the selected banks have this facility in their respective internet banking portals.

When any online transaction takes place through online banking, a SMS is sent to user's mobile phone to alert him about the transaction. All selected banks send mobile alert messages to their customer for online transactions. With this facility, online banking users may immediately notice, if any unauthorized transaction takes place.

The importance of passwords in today's online world is immense. We have to remember so many passwords but forgetting one can be a real headache. PNB, HDFC and ICICI banks offer the facility of generation of password online but in case of SBI Bank one has to visit the branch to request for new password. From convenience point, online generation of password is very good feature but there might be security concerns in this regard

There is always risk, if someone leaves online line banking portal unattended while logged in. In this case another person may use online banking portals in absence of genuine customer. Banks have introduced the facility of 'Idle Time log out' where user is automatically logged out after defined time. All selected banks' online portals have this feature.

There is another security feature of online banking portals i.e. Backspace' 'Fresh' 'Forward' logout where pressing of any of these buttons will result in automatically logout from the portal. All selected banks have this feature.

Section-II

5.2 SECURITY AND PRIVACY ISSUES IN E-BANKING : PERCEPTION OF BANK CUSTOMERS

A survey of 190 bank customers divided equally (Approximatly) among selected banks was conducted in the the Tri-city i.e Chandigarh UT, Mohali and Panchkula to understand the bank customers' perception towards 'security & privacy concern' and 'security & privacy satisfaction' regarding use of e-banking servcies. This section covers analysis of bank customers' perception towards 'security & privacy concern' and 'security & privacy satisfaction' regarding use of e-banking servcies i.e ATM, Internet Banking, Mobile Banking and Credit Cards.

5.2.1 Demographic profile of respondents

Demographic profile of surveyed respondents covering information on Gender, Age Groups (Years), Education, Occupation, Family Income, use of mobile phone and internet connection has been shown in Table 5.3.

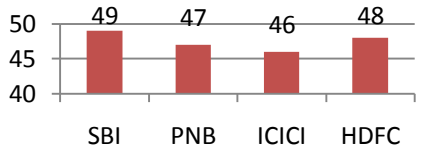
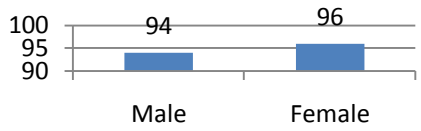
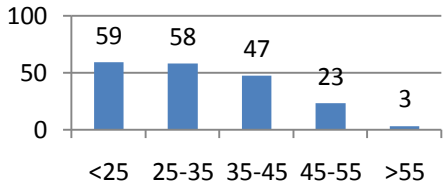
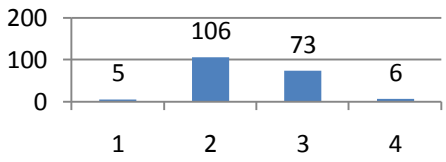
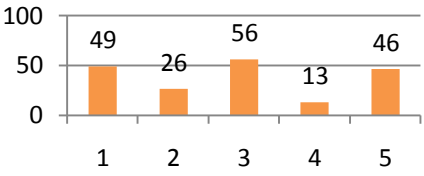
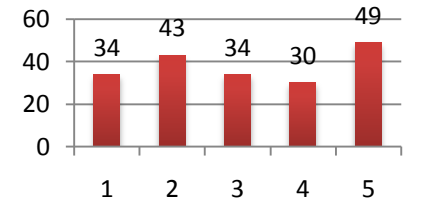
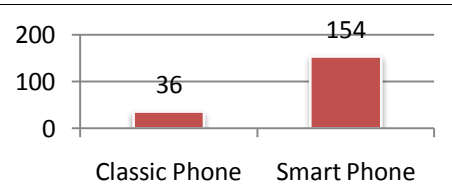
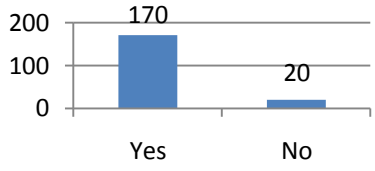
Bank-wise classification of respondents shows that maximum number of respondents were from SBI (25.8%) followed by HDFC Bank (25.3%), PNB (24.7%) and ICICI Bank (24.2%). Although, equal proportion was decided in the beginning of the study but this is the final distribution of respondents based on filled questionnaires received. Respondents were equally distributed on the basis of gender i.e. Male (49.5%) and Female (50.5%).

Age-wise distribution of respondents shows that majority of the respondents (61.6%) were from age groups 'Less than 25' (31.1%) and '25-35' (30.5%) taken together. It was followed by age groups '35-45' (24.7%), '45-55' (12.1%) and 'Above 55' (1.6%). Although, age distribution is skewed towards younger age groups but such age-wise distribution presents the glimpse about adoption of e-banking services in the tri-city. It is clearly visible that e-banking services are more popular among youngsters when compared with upper age groups.

Education- wise, majority of respondents (55.8%) were 'Graduate' followed by 'Post-Graduate' (38.4%), 'Others' (3.2%) and Undergraduate (2.6%). The category 'Others' included PhD and diploma holders. Occupation-wise, maximum number of respondents was servicemen (29.5%), followed by professionals (25.8%), students (24.2%), business persons (13.7%) and housewife (6.8%). Family income-wise distribution shows that maximum number of respondents were from income group 'More than Rs.100000' (25.8%) followed by 'Rs.40000-60000' (22.6%), 'less than Rs.80000'& '60000- 80000' (17.9%) and Rs. '80000- 100000' (15.8%).

Table 5.3
Demographic Profile of Respondents

N=190

Demographic	Frequency	Percentage	Graph
Bank			
HDFC	48	25.3	
ICICI	46	24.2	
PNB	47	24.7	
SBI	49	25.8	
Gender			
Male	94	49.5	
Female	96	50.5	
Age Groups (Years)			
Less than 25	59	31.1	
25-35	58	30.5	
35-45	47	24.7	
45-55	23	12.1	
Above 55	3	1.6	
Education			
Undergraduate (1)	5	2.6	
Graduate (2)	106	55.8	
Post graduate (3)	73	38.4	
Others (4)	6	3.2	
Occupation			
Professional (1)	49	25.8	
Business person (2)	26	13.7	
Service (3)	56	29.5	
House wife (4)	13	6.8	
Student (5)	46	24.2	
Family Income (Rs/Months)			
Less than 40000 (1)	34	17.9	
40000-60000 (2)	43	22.6	
60000-80000 (3)	34	17.9	
80000-100000 (4)	30	15.8	
> 100000 (5)	49	25.8	
Type of Mobile Phone			
Classic Phone	36	18.9	
Smart Phone	154	81.1	
Internet at Home			
Yes	170	89.5	
No	20	10.5	

It is the fact that mobile phone and internet are the major drivers of e-banking in India. In this context data was also sought form the respondents about type of mobile they were using and availability of internet connection at home. Table shows that vast majority of respondents had Smart phone (81.1%) which can be used for banking services besides other multimedia functions. Only 18.9 per cent of the respondents had classic phone i.e. the basis phone. Similarly, vast majority of respondents (89.5%) had internet connection at their homes. The information about these two variables has been further used in the analysis to study the usage pattern of e-banking services.

5.2.2 Respondents' Awareness of e-banking Services

At present, all commercial banks are offering majority of e-banking services. They spend huge amount on infrastructure and other ICT (*Information and communication technology)*. The first stage of adoption of these services is awareness of these services. Thus, awareness of e-banking services plays an important role in the adoption of these services. In this background, to understand the awareness level of respondents of e-banking services, they were asked to indicate their awareness about a given service i.e. ATM, Internet Banking, Mobile Banking and Phone Banking. Respondents' responses in this regard are shown in Table 5.4.

Table 5.4
Respondents' Awareness of E-Banking Services
(Bank-wise classification)

N=190

E-banking Services	Public Sector Banks		Private Sector Banks		Total
	SBI	PNB	ICICI	HDFC	
ATM	49 (100.0)	47 (100.0)	46 (100.0)	48 (100.0)	190 (100.0)
Internet Banking	46 (93.9)	30 (63.8)	46 (100.0)	46 (95.8)	168 (88.4)
Mobile Banking	27 (55.1)	19 (40.4)	27 (58.7)	35 (72.9)	108 (56.8)
Phone Banking	23 (46.9)	9 (19.1)	23 (50.0)	29 (60.4)	84 (44.2)
N	**49**	**47**	**46**	**48**	**190**

N represent number of bank customer surveyed.
Note: Figures within Parenthesis in this table and all the table to follow tables represent Percentages while figures without parentheses represent simple frequencies.

Figure 5.1: Awareness of E-Banking Services(%)

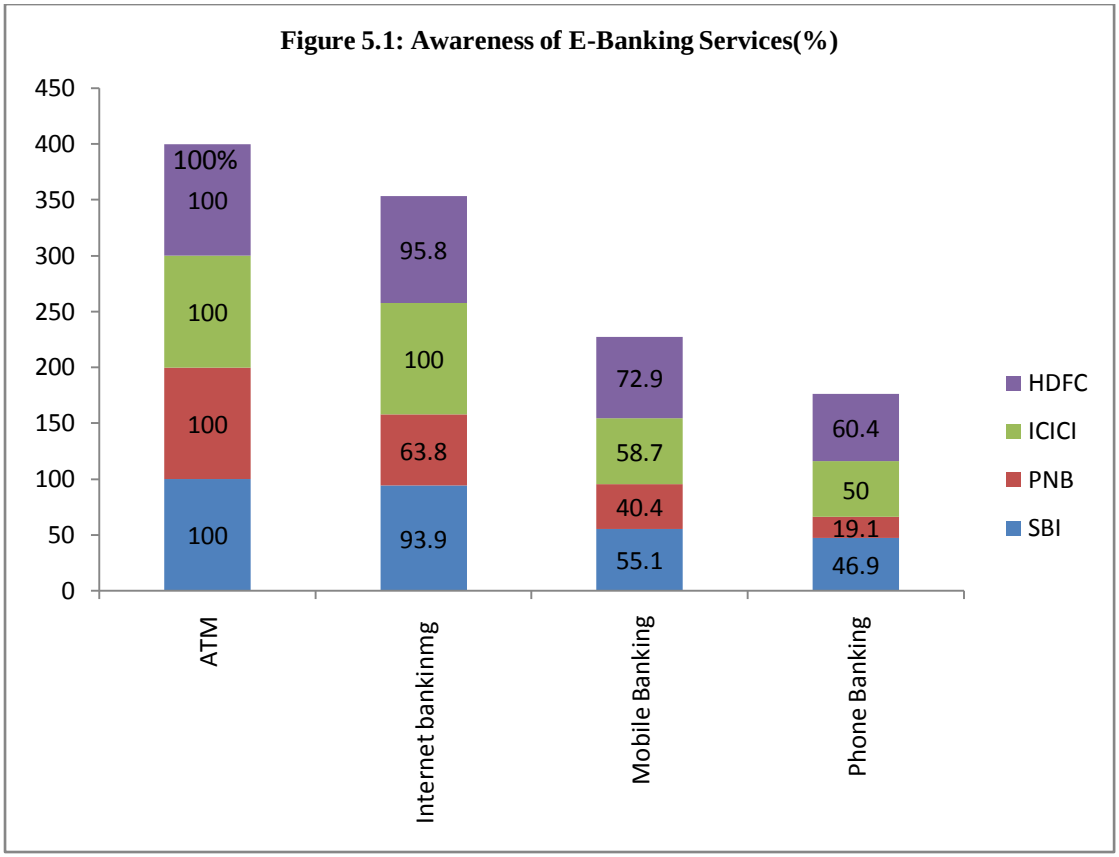


Table 5.4 shows that respondents' awareness of 'ATM' and 'Internet Banking' was very high as all the respondents in case of ATM and 88.4 per cent of respondents in case of Internet Banking were aware of these services. Furthermore, the awareness of Mobile Banking was quite good among respondents as 56.8 per cent of respondents were aware about it. However, only 44.2 per cent of respondents were aware of Phone Banking. The high awareness about ATM and Internet Banking may be attributed to the banks' efforts to spread the awareness about these channels among customers by using different methods of communication. Mobile banking has been recently started by the banks and customers may become aware about it with the passage of time. Phone banking was started long time back but awareness of this channel is little bit low as compared to other channels, may be because of more focus on latest e-banking services.

Bank- wise distribution of respondents on the basis of awareness shows that all the respondents irrespective of their banks were aware about ATM. All the respondents from ICICI Bank and more than ninety per cent of respondents from HDFC (95.8%) and SBI (93.9%) were aware of Internet Banking. These three banks were amongst few banks who started Internet Banking in India in the initial days of financial sector reforms. Similarly, high proportion of respondents from HDFC Bank (72.9%) were aware of Mobile Banking followed by respondents from ICICI Bank (58.7%) and SBI (55.7%), however, only 40.4 per cent of respondent form PNB were aware of Mobile Banking. As far as PNB is concerned, one of the reasons may be the late start of mobile banking by PNB amongst selected banks. Further, majority of respondents from HDFC bank (60.4%) and ICICI (50.0%) were aware of Phone Banking followed by respondents from SBI (46.9%). Only 19.1 per cent of respondent from PNB were aware of Phone Banking. Although PNB's website has no information about Phone banking but these respondents might be aware of phone banking because of their personal interest.

5.3 SECURITY AND PRIVACY ISSUES IN ATMs

The present study focuses on security and privacy issues in e-banking. In this context, bank customers' perception towards 'security and privacy concern' and 'security and privacy satisfaction' has been analyzed for various e-banking services. This part of the study deals with respondents' opinion about security and privacy issues in ATM**.** Respondents were asked about duration of ATM use, frequency of using ATM, security and privacy concern regarding ATM use and security and privacy satisfaction regarding ATM use.

5.3.1 Duration and Frequency of ATM use

Respondents were asked about their duration and frequency of ATM use. Table 5.5 and 5.6 depict duration and frequency of ATM use by the customers of selected banks.

Table 5.5
Duration of ATM Use
(Bank-wise classification)

N=190

Duration of Use (Years)	Public Sector Banks		Private Sector Banks		Total
	SBI	PNB	ICICI	HDFC	
Less than 1	2 (4.1)	1 (2.1)	0 (0.0)	1 (2.1)	4 (2.1)
1-2years	4 (8.2)	9 (19.1)	1 (2.2)	1 (2.1)	15 (7.9)
2-4years	7 (14.3)	14 (29.8)	7 (15.2)	13 (27.1)	41 (21.6)
4-6 years	14 (28.6)	6 (12.8)	13 (28.3)	7 (14.6)	40 (21.1)
More than 6 years	22 (44.9)	17 (36.2)	25 (54.3)	26 (54.2)	90 (47.4)
N	**49**	**47**	**46**	**48**	**190**

Table 5.5 shows that all the respondents were using ATM irrespective of their banks. Duration-wise, maximum number of respondents had been using ATM for more than six years (47.4%) followed by duration categories '2-4 years' (21.6%), '4-6 years' (21.2%), '1-2 years' (7.9%) and 'less than 1year' (2.1%). It is evident that majority of respondents had been using ATM service for reasonable duration i.e. more than 4 years. Bank-wise distribution shows that in case of all the selected banks, maximum proportion of respondents had been using ATM for more than six years. It was followed by '4-6 years' in case of SBI (28.6%) & ICICI (28.3%) and '2-4 years' in case of PNB (29.8%) & HDFC (27.1%). Very small proportion of respondents from all the banks had been using ATM for less than one year.

Table 5.6
Frequency of ATM Use
(Bank-wise classification)

N-190

Frequency of Usages (Years)	**Public Sector Banks**		**Private Sector Banks**		**Total**
	SBI	**PNB**	**ICICI**	**HDFC**	
More than once in a week	15 (30.6)	9 (19.1)	13 (28.3)	14 (29.2)	51 (26.8)
Once in a week	13 (26.5)	21 (44.7)	10 (21.7)	11 (22.9)	55 (28.9)
Once in a Fortnight	17 (34.7)	4 (8.5)	16 (34.8)	20 (41.7)	57 (30.0)
Once in a month	1 (2.0)	13 (27.7)	6 (13.0)	2 (4.2)	22 (11.6)
Once in a quarter	3 (6.1)	0 (0.0)	1 (2.2)	1 (2.1)	5 (2.6)
N	49	47	46	48	190

Table 5.6 highlights that maximum number of respondents has been using ATM 'Once in a Fortnight' (30.0%) followed by 'Once in a week' (28.9%), and 'More than once in a week' (26.8%). Only 11.6 per cent and 2.6 per cent of respondents were using ATM 'once in a month' and 'once in a quarter' respectively. It seems from the above table that customers use ATM very frequently to conduct the banking transaction. Bank-wise analysis shows that maximum proportion of respondents from banks; SBI (34.7%), ICICI (34.8%) and HDFC (41.7%) use ATM 'once in a Fortnight' followed by 'once in a week'. However, in case of PNB maximum proportion of respondents use ATM 'once in a week' (44.7%) followed by 'once in a month (27.7%). Further, very small proportion of respondents from all the banks was using ATM 'once in a quarter'.

5.3.2 Perception toward 'Security and Privacy Concern' regarding use of ATM

To measure bank customers' perception towards 'security and privacy concern' regarding use of ATM, a self developed 9 items *'Security and Privacy*

Concern: ATM' construct was used. Respondents were asked to indicate their opinion about given statements on Five point Likert Scale ranging from 'Strongly Agree' to 'Strongly Disagree'. The statements on different aspects of 'security and privacy concerns' were designed in such a way that agreeableness to a statement would reflect higher concern for a given aspect of security and privacy or vice versa. Further, mean scores have been calculated for each statement by assigning weights of 5,4,3,2 and 1 to 'Strongly Agree', 'Agree', 'Neutral', 'Disagree' and 'Strongly Disagree'. The level of security and privacy concern was measured by calculating Grand Mean. Descriptive and bank-wise respondents' perception towards security and privacy concern' regarding use of ATMs have been shown in Table 5.7 and Table 5.8 respectively.

Table 5.7
Security and Privacy Concern Regarding Use of ATM
(Descriptive Statistics)

N=190

Item Code	Statement	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	Mean± SD
ATMC1	My ATM PIN may be stolen	18	58	39	58	17	2.99±1.164
ATMC2	My ATM card maybe cloned (duplicated)	23	30	48	73	16	3.15±1.161
ATMC3	My ATM may dispense less amount of currency than requested by me	51	65	29	39	06	2.39±1.176
ATMC4	Someone may withdraw cash from my ATM without using my card	38	86	25	36	05	2.39±1.087
ATMC5	Someone can transfer cash from my ATM without using my card	35	82	40	25	08	2.42±1.064
ATMC6	There may be deduction in my balance without any transaction	23	74	40	47	06	2.68±1.073
ATMC7	My card information may be shared by the bank with Third party	41	53	40	42	14	2.66±1.245
ATMC8	Others may see my password while entering it	30	20	50	72	18	3.15±1.217
ATMC9	I will not get my card back if stuck in ATM	33	54	49	40	14	2.73±1.190
Mean score of Security and Privacy Concern		2.7275 ±.75701					

Table 5.7 shows that respondents were moderately concerned about ATM's security and privacy (2.7275±.75701). However, statement-wise analysis shows that respondents had shown 'high' level of concern towards possibility of cloning of their ATM cards (ATMC1, 3.15±1.16), possibility that others may see ATM password (PIN) while entering it (ATMC8,3.15±1.217) and chances of stealing ATM PIN (ATMC1, 2.99±1.164). Respondents' concern level was 'moderate' towards stucking of ATM card (ATMC9, 2.73±1.190), deduction in balance without transaction (ATMC6, 2.68±1.073), sharing of card information by the bank with others (ATMC7, 2.66±1.245), dispense of less amount from ATM (ATMC3, 2.39±1.176), withdrawal of amount without using card (ATMC4, 2.39±1.087) and transfer of cash from ATM without using card (ATMC5, 2.42±1.064).

The analysis of respondents' opinion in this regard shows that cloning of ATM card was the major issue of concern for ATM users. This may be attributed to frequent news articles of ATM frauds appearing in the local newspapers of Tri–city national level newspapers. Further, cloning of ATM card has become the very common way of ATM frauds. Majority of the ATM frauds have been committed with the help of cloning of cards only. A recent news article shows that "In the last two months, the UT Police has registered nearly 60 cases of ATM card cloning resulting in a loss of thousands of rupees to the account holders. Surprisingly, in the majority of cases, the cloning was done after the complainants had used the debit/credit card to make a payment at a petrol pump"[20] Thus, respondents' concern seems to be genuine in this regard. Further, respondents' concern that others can see their ATM password (PIN) while entering it, may be justified that it is quite possible for others to see the

[20] Indian Express, Chandigarh, Wed Mar 13 2013, 02:51 hrs.

password by a person standing in queue just behind, if you have very casual approach when interacting with ATM.

Table 5.8
Security and Privacy Concern Regarding Use of ATM
(Bank-wise classification)

N=190

Item Code	Statement	Public Sector Banks		Private Sector Banks		ANOVA Statistic DF (3,186)	
		SBI	PNB	ICICI	HDFC	F-Value	P-value
ATMC1	My ATM password may be stolen	3.1837	2.8511	2.8261	3.0833	1.084	.357
ATMC2	My ATM card maybe cloned (duplicated)	3.3265	2.8723	3.0217	3.3750	2.099	.102
ATMC3	My ATM may dispense less amount of currency than requested by me	2.3673	1.9574	2.4565	2.7708	4.042	.008*
ATMC4	Someone may withdraw cash from my ATM without using my card	2.6531	1.8936	2.3696	2.6250	5.322	.002*
ATMC5	Someone can transfer cash from my ATM without using my card	2.5510	2.0213	2.4565	2.6250	3.161	.026*
ATMC6	There may be deduction in my balance without any transaction	2.8980	2.4468	2.4348	2.9167	3.095	.028*
ATMC7	My card information may be shared by the bank with Third party	2.7959	2.0426	2.3913	3.3750	11.762	.000*
ATMC8	Others may see my password while entering it	3.3878	2.7234	2.8478	3.6042	6.195	.000*
ATMC9	I will not get my card back if stuck in ATM	2.6327	2.4468	2.5435	3.2708	4.970	.002*
Mean score of Security and Privacy Concern		2.8662	2.3617	2.5942	3.0718	9.006	.000*

Significant at 5% level (.05).

Table 5.8 shows that overall level of security and privacy concern regarding use of ATM is highest among respondents of HDFC bank (3.0718) followed by respondents from SBI (2.8662), ICICI (2.5942) and PNB (2.3617). ANOVA result shows that there was significant difference in the bank customers' perception towards security and privacy concern regarding use of ATMs across selected banks [F (3,186) = 9.006, p=0.00]. Thus, Null hypothesis $H_0$1 is rejected.

Figure 5.2: Level of 'Security and Privacy' concern (ATMs)

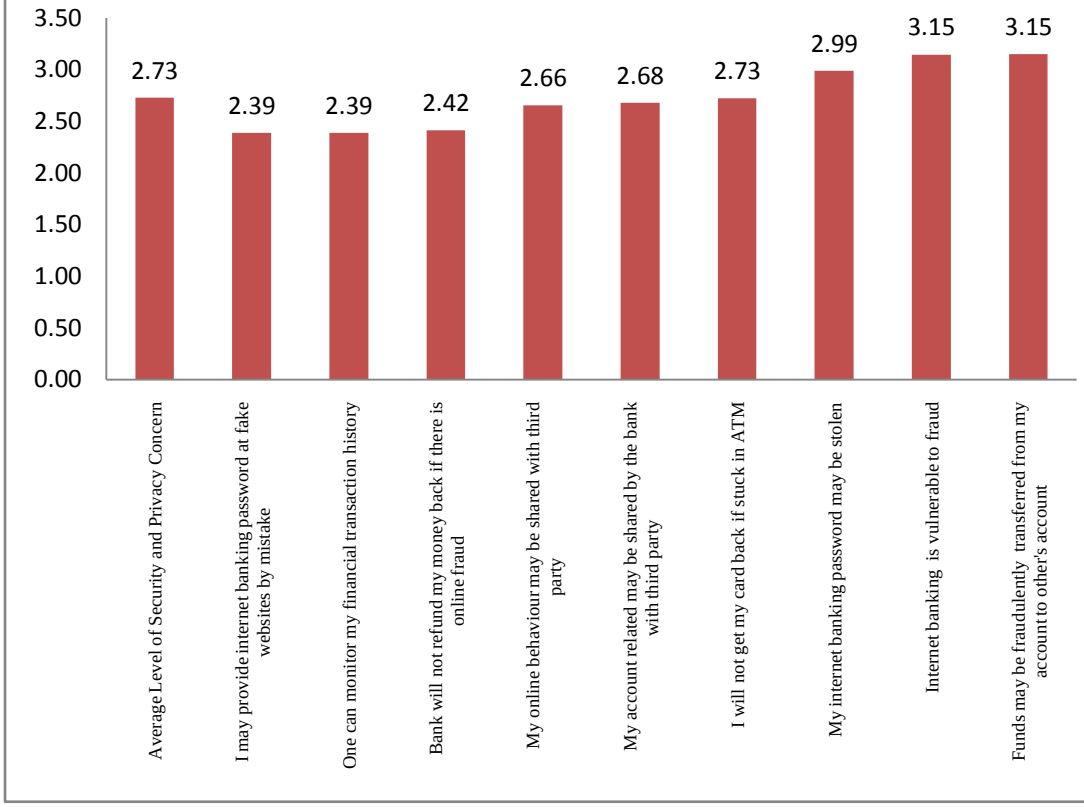
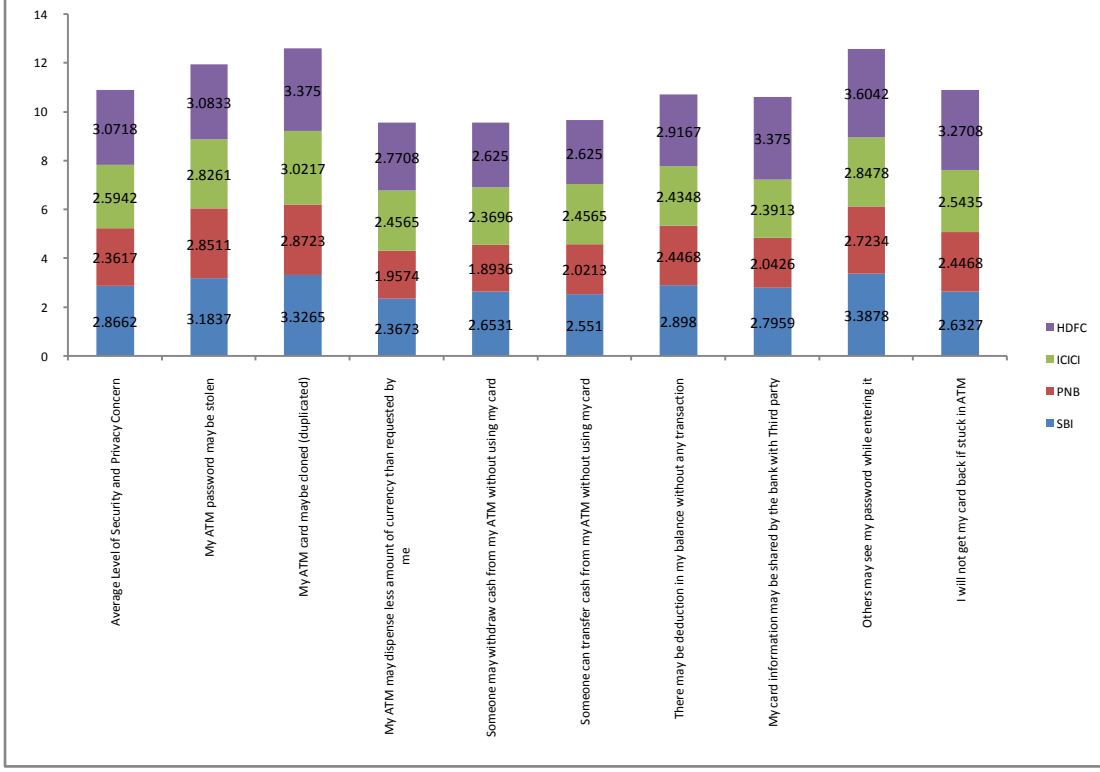


Figure 5.3: Bank-wise level of 'security and privacy concern'(ATMS)



Further, analysis of each statement shows that respondents concern depicted through statements ATMC2, ATMC3, ATMC5, ATMC6, ATMC7, ATMC8 and ATMC9 was highest in case of HDFC followed by SBI. On the other hand, respondents' concern depicted through statement ATMC1 and ATMC4 was highest in case of SBI followed by HDFC.

One way ANOVA results shows that there was significant difference in the bank customers' perception towards security and privacy concern regarding use of ATMs across selected banks with respect to items ATMC3 [F (3,186)=4.042, p=0.08], ATMC4[F (3,186)=5.322, p=.002], ATMC5 [F (3,186)=3.161, p=.026], ATMC6[F (3,186) = 3.095, p=.028, ATMC7 [F (3,186) =11.762, p=000], ATMC8 [F (3,186) = 6.195, p=0.00] and ATMC9 [F (3,186)=4.970, p=0.02]. For rest of the statements there was no significant difference in the bank customers' perception towards security and privacy concern regarding use of ATMs across selected banks.

5.3.3 Perception toward Security and Privacy satisfaction regarding use of ATM

To measure bank customers' perception towards 'security and privacy satisfaction' regarding use of ATM, a self developed 10 items *'Security and Privacy satisfaction: ATM'* construct was used. Respondents were asked to indicate their opinion about given statements on Five point Likert Scale ranging from 'Strongly Agree' to 'Strongly Disagree'. The statements on different aspects of security and privacy satisfaction were designed in such a way that agreeableness to the statement would reflect the higher satisfaction for given aspect or vice versa. Further, mean scores have been calculated for each statement by assigning weights of 5,4,3,2 and 1 to 'Strongly Agree', 'Agree', 'Neutral', 'Disagree' and 'Strongly Disagree'. The level of Security and Privacy satisfaction has been measured by taking the Grand Mean of all the statements'. Descriptive and bank- wise security and privacy satisfaction regarding ATM use have been shown in Table 5.9 and Table 5.10 respectively.

Table 5.9

Descriptive of Security and Privacy satisfaction level regarding use of ATM

N=190

Item Code	Statement	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	Mean± SD
ATMS1	It is safe to withdraw the cash from my banks' ATMs	0	3	22	131	34	4.03±.599
ATMS2	My PIN can't be hacked while using my banks' ATMs	8	49	62	64	7	3.07±.954
ATMS3	It is not possible for others to see my password while entering	1	73	62	43	11	2.95±.930
ATMS4	My ATM card can't be cloned (Duplicated)	8	75	61	33	13	2.83±.994
ATMS5	My Bank guides me about security tips from time to time	6	56	48	64	16	3.15±1.039
ATMS6	There is limit of maximum number of incorrect password submissions	2	9	32	113	34	3.88±.788
ATMS7	Contact information is easily available to block my ATM card	2	32	41	86	29	3.57±.978
ATMS8	Door of the ATM Cabin has secure access	32	77	27	33	21	2.65±1.258
ATMS9	There is adequate privacy while using ATM	13	65	54	38	20	2.93±1.113
ATMS10	Only one person is allowed to enter ATM Cabin for transaction.	17	70	26	50	27	3.00±1.251
Security and Privacy Satisfaction Level		3.2063±.4842					

Table 5.9 shows that respondents' overall satisfaction level of ATMs' security and privacy was 'high' (3.2063±0.4842). Statement-wise analysis shows that respondent's satisfaction level regarding safety of withdrawal of cash from ATM (ATMS1, 4.03±.599) was 'very high' and it was highest among given statements. It was followed by satisfaction about limit of maximum number of incorrect password submissions (ATMS6, 3.88±.788), availability of contact information to block ATM card (ATMS7, 3.57±.978), guidance about security tips (ATMS5, 3.15±1.039), Safety of PIN (ATMS2, 3.07±.954), entry of one person in ATM cabin (ATM10, 3.00±1.251) where level of satisfaction was found 'high'. 'Moderate' level of satisfaction was found in case of privacy of password (ATMS3, 2.95±.930), privacy while using ATM (ATMS9, 2.93±1.113), Cloning of ATM card (ATMS4, 2.83±.994), and secure access of ATM doors (ATMS8, 2.65±1.258). One inference might be drawn from Table 5.7 and 5.9 that although, respondent are satisfied about most of the security and privacy aspects of ATMs but still the concern is there in the minds of

customers about ATMs. It seems that respondents' concern has somewhere impacted their satisfaction level regarding use of ATM too. Respondents showed higher level of concern about cloning of cards (Table 5.7), similarly their satisfaction level about cloning of cards.

Table 5.10
Security and Privacy satisfaction level regarding use of ATM
(Bank-wise classification)

N=190

Item code	Statement	Public Sector Banks		Private Sector Banks		ANOVA Statistic Df(3,186)	
		SBI	PNB	ICICI	HDFC	F-Value	P-value
ATMS1	It is safe to withdraw the cash from my banks' ATMs	4.1429	4.2553	3.9565	3.7708	6.553	.000*
ATMS2	My PIN can't be hacked while using my banks' ATMs	3.0204	3.3404	3.0000	2.9167	1.821	.145
ATMS3	It is not possible for others to see my password while entering	2.8980	3.1277	2.9348	2.8333	0.877	.454
ATMS4	My ATM card can't be cloned (Duplicated)	2.8776	3.0000	2.6304	2.8125	1.121	.342
ATMS5	My Bank guides me about security tips from time to time	3.6327	2.6596	3.2609	3.0208	8.305	.000*
ATMS6	There is limit of maximum number of incorrect password submissions	3.7755	3.7021	4.1304	3.9375	2.793	.042*
ATMS7	Contact information is easily available to block my ATM card	3.4082	3.6170	3.6739	3.5833	.656	.580
ATMS8	Door of the ATM Cabin has secure access	2.7959	2.7021	2.7826	2.3333	1.441	.232
ATMS9	There is adequate privacy while using ATM	3.0612	3.2128	2.8261	2.6250	2.640	.051
ATMS10	Only one person is allowed to enter ATM Cabin for transaction.	2.8980	3.5957	2.5435	2.9583	6.188	.000*
Security and Privacy Satisfaction Level		3.2510	3.3213	3.1739	3.0792	2.237	.085

Significant at 5% level (.05)

Table 5.10 shows that among selected banks, respondents' security and privacy satisfaction level regarding use of ATMs was 'high' in case of all the selected banks i.e. PNB (3.3213), SBI (3.2510), ICICI (3.1739) and HDFC(3.0792). However, One way ANOVA test shows that there was no significant difference in the bank customers' perception towards 'security and privacy satisfaction' regarding use of ATMs across selected banks [F (3,186) =2.237, p=.085]. Thus, Null hypothesis $H_0 2$ is accepted.

Figure 5.4: Level of 'Security and Privacy' satisfaction (ATMs)

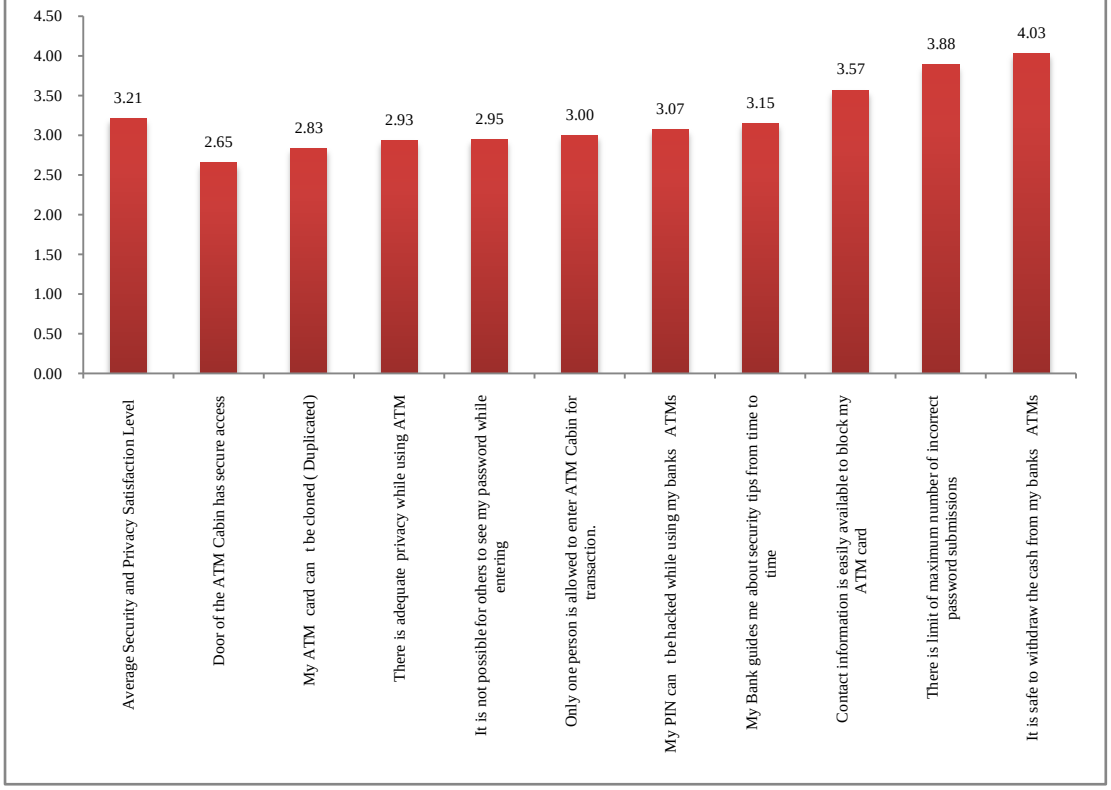
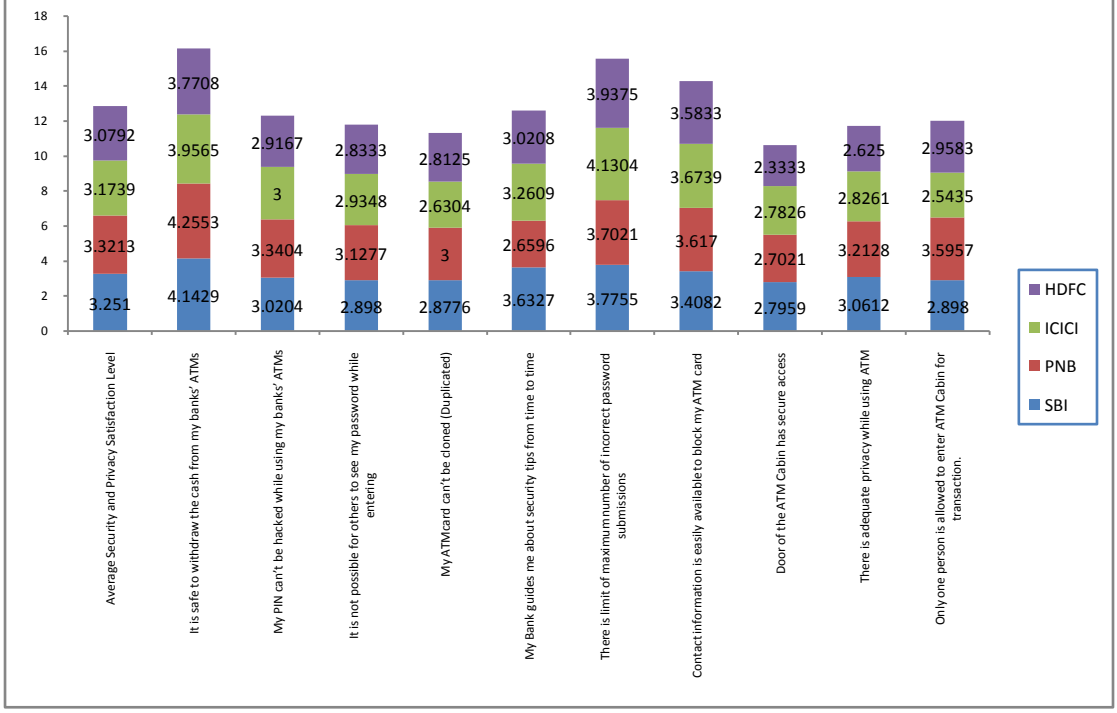


Figure 5.5: Bank-wise level of 'security and privacy' satisfaction (ATMS)



Items wise analysis shows that respondents of PNB were more satisfied regarding security and privacy aspects depicted through statements ATMS1 (4.2553), ATMS2 (3.3404), ATMS3 (3.1277), ATMS4 (3.0000) ATMS9 (3.2128) and ATMS10 (3.5957) when compared with other banks. Similarly, respondents from SBI were more satisfied with items ATMS5 (3.6327) and ATMS8 (2.7959). Further, respondents from ICICI and HDFC were more satisfied with items ATMS6 (4.1304) and ATMS7 (3.5833) respectively when compared with other banks. One way ANOVA test shows that there is significant difference in the bank customers' perception towards security and privacy satisfaction regarding use of ATMs across selected banks with respect to items; ATMS1 [F(3,186)=6.553, p=0.00], ATMS5 [F (3,186)=8.305, p=0.00], ATMS6 [F(3,186)=2.793, p=.042] and ATM10 [F(3,186)=6.188, p=0.00).

5.3.4 Relationship between Security & Privacy Concern and satisfaction level (ATM)

To establish the relationship between bank customers' perception regarding 'Security & Privacy Concern' and 'Security & Privacy Satisfaction' regarding use of ATM, Pearson's coefficient of correlation was calculated (Table 5.11).

Table 5.11
Correlation between Security & Privacy Concern and Security & Privacy Satisfaction Level (ATM)

Pearson Correlation	r	p
	-.175*	.016
N	190	

Significant at .05

Table 5.11 shows that there is a negative and significant correlation between bank customers' perception of 'security & privacy concern' and 'security & privacy satisfaction' in case of ATM use [r (190) =-.175, p=.016)]. Thus, null hypothesis $H_0$3

is rejected. It is evident that in case of ATM, with the increase in Security & Privacy Concern, the level of Security & Privacy Satisfaction will decrease or vice versa.

5.4 SECURITY AND PRIVACY ISSUES IN INTERNET BANKING

Internet Banking is becoming popular among bank customers but still many customers hesitate to adopt it. There might be number of reasons for it, however, security and privacy has been cited as the major roadblock by majority of the studies. Thus, this part of the study analyses the security and privacy issues regarding the use of Internet Banking. Respondents were asked questions about Adoption, Frequency and Purpose of Internet Banking. Further respondents' concern and satisfaction level regarding use of internet banking has been measured.

5.4.1 Adoption, Frequency and Purpose of using Internet Banking

With the purpose of exploring adoption and usage behavior, respondents were asked about their adoption, frequency and purpose of using internet banking. Respondents' responses have been shown in Table 5.12, Table 5.13 and Table 5.14 respectively.

Table 5.12
Adoption of Internet Banking
(Bank-wise Classification)

N=190

Response	Public Sector Banks		Private Sector Banks		Total
	SBI	PNB	ICICI	HDFC	
Yes	42 (85.7)	20 (42.6)	42 (91.3)	38 (79.2)	142 (74.7)
No	7 (14.3)	27 (57.4)	4 (8.7)	10 (20.8)	48 (25.3)
Total	49	47	46	48	190

Table 5.12 shows that out of 190 surveyed bank customers, 74.7 per cent were using internet banking. Bank wise classification shows that maximum number of

respondents from ICICI Bank (91.3%) was Internet Banking users. It was followed by respondents from HDFC (79.2%), SBI (85.7%) and PNB (42.6%).

Table 5.13 shows the frequency of use of internet banking by bank customers of selected banks.

Table 5.13
Frequency of Internet Banking Use
(Bank-wise classification)

N=142

Frequency of Usages (Years)	**Public Sector Banks**		**Private Sector Banks**		**Total**
	SBI	PNB	ICICI	HDFC	
More than once in a week	4 (9.5)	1 (5.0)	12 (28.6)	2 (5.3)	19 (13.4)
Once in a week	6 (14.3)	0 (0.00)	6 (14.3)	9 (23.7)	21 (14.8)
Once in Fortnight	6 (14.30)	4 (20.0)	12 (28.6)	12 (31.6)	34 (23.9)
Once in a month	20 (47.6)	10 (50.0)	10 (23.8)	13 (34.2)	53 (37.3)
Once in a quarter	6 (14.3)	5 (25.0)	2 (4.8)	2 (5.3)	15 (10.6)
N	**42**	**20**	**42**	**38**	**142**

Table 5.13 shows that maximum number of respondents had been using Internet banking ‘once in a month’ (37.3%) followed by ‘Once in Fortnight’ (23.9%), Once in a week (14.8%), More than once in a week’ (13.4%), and ‘Once in a Quarter’ (10.6%). The data reveals that respondents were using internet banking frequently to conduct banking transactions. Bank-wise analysis shows that highest proportion of respondents from SBI (47.67%), PNB (50.0%), and HDFC (34.2%) had been using internet banking ‘Once in a month’. On the other hand, highest proportion of respondents from ICICI (28.6% each) was using Internet Banking ‘Once in fortnight’ and ‘More than once in a week’. Moreover, it is visible from the data that frequency of using internet banking is more among respondents of Private sector banks as compared respondents from Public sector banks.

Internet banking may be used to perform number of banking transactions. To know about the usages pattern of internet banking, respondents were asked about the purpose of using internet banking (Table 5.14).

Table 5.14
Purpose of Using Internet Banking
(Bank- wise Classification)

N=142

Purpose	Public Sector Banks		Private Sector Banks		Total
	SBI	PNB	ICICI	HDFC	
Checking of Balance	27 (64.3)	10 (50.0)	29 (69.0)	29 (76.3)	95 (66.90)
Checking of Mini Statement	22 (52.4)	14 (70.0)	32 (76.2)	22 (57.9)	90 (63.38)
Transfer of Funds	25 (59.5)	10 (50.0)	30 (71.4)	22 (57.9)	87 (61.27)
Payment of Bills	23 (54.8)	12 (60.0)	33 (78.6)	22 (47.4)	90 (63.38)
Online shopping	23 (54.8)	12 (60.0)	33 (78.6)	35 (92.9)	103 (72.55)
N	**42**	**20**	**42**	**38**	**142**

Table 5.14 highlights very interesting fact that 72.55 per cent of respondents were using Internet Banking for online shopping, which is highest among given options. It was followed by 'Checking of Balance' (66.90%), 'Checking of Mini Statement' (63.38%), Payment of Bills (63.38%) and 'Transfer of Funds' (61.27%). The wide use of internet banking for online shopping may be because of the simple procedure which a user has to follow while making payments. The procedure for making online payments through internet banking is simple than other online payment methods. Bank-wise analysis shows that maximum proportion of respondents from HDFC (92.9%) use internet banking for online shopping followed by ICICI (78.6%), PNB (60%) and SBI (54.8%). Further, 78.7 per cent of respondents from ICICI bank use internet banking for 'Payment of Bill' followed by PNB (60.0%), SBI (54.8%), and HDFC (47.4%). Similarly, maximum proportion of respondents from ICICI (71.4%) use 'Transfer of Funds' facility followed by SBI (59.5%), HDFC (57.9%) and PNB (50.0%). Moreover, maximum proportion of respondent from HDFC and

ICICI used internet banking for 'Checking of Mini Statement' and 'Checking of Balance' respectively. It is evident that transactional functions of internet banking were used more by the respondents of private banks.

5.4.2 Strength of password and Awareness of IB security features

To know the opinion about strength of internet banking password, respondents were asked to indicate the strength of password on Five Point Likert scale ranging from 'Very Strong' to 'Very Weak' (Table 5.15).

Table 5.15
Respondents' Opinion about Strength of Password
(Bank- wise Classification)

N=142

Strength of password	Public Sector Banks		Private Sector Banks		Total
	SBI	PNB	ICICI	HDFC	
Very Strong	25 (59.5)	2 (10.0)	16 (38.1)	30 (78.9)	73 (51.4)
Strong	17 (40.5)	18 (90.0)	26 (61.9)	8 (21.9)	69 (48.6)
Neither Weak Nor Strong	0 (0.0)	0 (0.0)	0 (0.0)	0 (0.0)	0 (0.0)
Weak	0 (0.0)	0 (0.0)	0 (0.0)	0 (0.0)	0 (0.0)
Very Weak	0 (0.0)	0 (0.0)	0 (0.0)	0 (0.0)	0 (0.0)
N	**42**	**20**	**42**	**38**	**142**

Table 5.15 shows that majority of respondents were of opinion that their internet banking password was 'very strong' (51.4%) followed by 'strong' (48.6%). Interestingly, none of the respondent opined that he or she had weak password. Same trend was observed bank-wise also. It shows that banks have been providing option to the customers to set their password very strong and customers make use this facility.

The basic awareness about internet banking features plays an important role in the security of internet banking. Respondents were asked about their awareness of basic security features of internet banking (Table 5.16).

Table 5.16
Awareness about Internet Banking Security Features
(Bank- wise Classification)

N=142

Internet Banking Security Features	Public Sector Banks		Private Sector Banks		Total
	SBI	PNB	ICICI	HDFC	
One time password (OTP)	30 (71.4)	15 (75.0)	36 (85.7)	38 (100)	119 (83.80)
Profile password	25 (59.5)	2 (10.0)	16 (38.1)	30 (78.9)	73 (51.40)
Hyper Text Transfer Protocol secured (https)	15 (35.7)	15 (75.0)	25 (59.5)	17 (44.7)	72 (50.70)
Virtual key board	32 (76.2)	19 (76.2)	39 (92.9)	35 (92.1)	125 (88.02)
N	**42**	**20**	**42**	**38**	**142**

Table 5.16 depicts that vast majority of respondents were aware of 'Virtual Keyboard' (88.02%) and 'One time password' (83.80%). Similarly, majority of respondents were aware of 'Profile password' (51.40%) and Hyper Text Transfer Protocol secured (https) (50.70%). It shows that customers were quite aware about internet banking security features. Bank-wise analysis shows that respondent across all the banks were well aware of internet banking security features except Profile password in case of PNB (10.0%) & ICICI (38.1%) and Hyper Text Transfer Protocol secured in case of SBI (35.7%) and HDFC (44.7%) where the proportion of respondent is lesser The reason for low awareness of Profile password may be attributed to use of different terms in place of it. Similarly, low awareness about Hyper Text Transfer Protocol Secured may be because of respondent's general knowledge.

5.4.3 Use and Awareness of virtual key Board

It is easy for fraudsters to hack internet banking password by capturing keystrokes on keyboard. This is possible through couple of programmes called 'Spy Ware', 'Trojan Programmes' and 'key-loggers' which are primarily designed to capture the key strokes (ET Bureau Feb 17, 2011, 01.39am IST). Virtual keypad is an

online application, which substitutes the actual physical keyboard with a mouse. When user clicks on the virtual keyboard option at the time of net banking, the monitor flashes a keyboard on screen. User has to use the mouse to click on the relevant keys to sign into net banking ID. Banks have come in with 'Virtual Keyboard' to protect the account and password information (IPINs) from fraudsters. Respondents were asked about the frequency of using virtual key board. (Table: 5.17)

Table 5.17
Use of Virtual Key Board
(Bank-wise Classification)

N=125

Frequency	Public Sector Banks		Private Sector Banks		Total
	SBI	PNB	ICICI	HDFC	
Never	11 (34.4)	8 (42.1)	11 (28.2)	6 (17.1)	36 (28.8)
Sometimes	11 (34.4)	7 (36.8)	19 (48.7)	17 (48.6)	54 (43.2)
Frequently	7 (21.9)	0 (0.00)	5 (12.8)	3 (8.6)	15 (12.0)
Always	3 (9.4)	4 (21.1)	4 (10.3)	9 (25.7)	20 (16.0)
N	**32**	**19**	**39**	**35**	**125**

Table 5.17 shows that only 16.0 per cent of respondents used virtual key board ‘Always’ and only 12.0 per cent used it ‘Frequently’. Further, 43.2 percent used virtual key board ‘Sometimes’ and 28.6 percent of respondent never used it. It is clear that despite of importance of virtual key board, the use of it is not very encouraging. Bank wise, analysis shows that 25.7 percent of respondents from HDFC used virtual key board ‘Always’ followed by respondents from PNB (21.1%), ICICI (10.3%) and SBI (9.4%). The proportion of virtual key board users was highest in case of SBI who use it frequently (21.9%). On the other hand, 42.1 percent of respondent from PNB never used virtual key board. It was followed by respondents from SBI (34.4%), ICICI (28.2%) and HDFC (17.1%).

Recently, banks have introduced two new types of virtual key board i.e. Scrambled Virtual Key Board, Hovering Virtual Key Board. Awareness regarding these two has been shown in Table 5.18.

Table 5.18
Awareness about New Types of Virtual Key Board
(Bank-wise Classification)

N=125

Type of Virtual Key Board	Public Sector Banks		Private Sector Banks		Total
	SBI	PNB	ICICI	HDFC	
Scrambled Virtual Key Board	18 (56.2)	7 (36.8)	19 (48.7)	10 (28.6)	54 (43.2)
Hovering Virtual Key Board	9 (28.1)	6 (31.6)	13 (33.3)	14 (40.0)	42 (33.6)
N	32	19	39	35	125

Table 5.18 shows that 43.2 percent of respondents and 33.6 per cent of respondents were aware of 'Scrambled Virtual Key Board' and 'Hovering Virtual Key Board' respectively. Bank-wise analysis shows that majority of respondents form SBI (56.2%) was aware of 'Scrambled Virtual Key Board' followed by ICICI (48.7%), PNB (36.8%) and HDFC (28.6%). Further, 40.0 percent of respondents from HDFC were aware of Hovering Virtual Key Board followed by ICICI (33.3%), PNB (31.6%) and SBI (28.1%). Although among selected banks only HDFC's online banking portal has 'Hovering Virtual Key Board' but awareness of it among respondents of other banks might be attributed general awareness.

5.4.4 Perception towards Security and privacy concern regarding use of Internet Banking

To measure the bank customers' perception towards 'security and privacy concern' regarding use of internet banking, a self developed 8 items *'Security and Privacy Concern: Internet Banking'* construct was used. Respondents were asked to indicate their opinion about given statements on Five point Likert Scale ranging from 'Strongly Agree' to 'Strongly Disagree'. The statements on different aspects of

security and privacy concerns were designed in such a way that agreeableness to the statement would reflect the higher concern for given aspect or vice versa. Further, mean scores have been calculated for each statement by assigning weights of 5,4,3,2 and 1 to 'Strongly Agree', 'Agree', 'Neutral', 'Disagree' and 'Strongly Disagree'. Level of security and privacy concern has been measured by taking Grand Mean of all the statements. Descriptive statistics and bank-wise customers' perception towards 'security and privacy concern' regarding use of Internet banking have been shown in Table 5.19 and Table 5.20 respectively.

Table 5.19
Security and Privacy Concern Regarding Use of Internet Banking
(Descriptive statistics)

N=142

Item Code	Statement	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	Mean± SD
IBC1	My internet banking password may be stolen	9	49	23	47	14	3.06±1.153
IBC2	Funds may be fraudulently transferred from my account to other's account	9	49	33	42	9	2.95±1.074
IBC3	I may provide internet banking password at fake websites by mistake	21	41	15	61	4	2.90±1.193
IBC4	One can monitor my financial transaction history	8	33	36	52	13	3.20±1.075
IBC5	Bank will not refund my money back if there is online fraud	12	14	57	49	10	3.22±1.011
IBC6	My account related may be shared by the bank with third party	12	53	36	35	6	2.79±1.044
IBC7	My online behaviour may be shared with third party	13	41	25	51	12	3.06±1.166
IBC8	Internet banking is vulnerable to fraud	3	15	31	69	24	3.68±0.949
Level of Security and Privacy Concern		3.1065 ±.72780					

Table 5.19 shows that in general respondents' level of security and privacy concern regarding use of internet banking was high (3.1065±.72780). Statement wise analysis shows that respondents had highest level of concern with respect to vulnerability of fraud in Internet (IBC8, 3.68±0.949) followed by concern about password hacking (IBC1, 3.06±1.153) , sharing of online behaviour with third party (IBC, 3.06±1.166), non refund of money in case of fraud (IBC5, 3.22±1.011), monitoring of financial transaction history (IBC4, 3.20±1.075), fraudulently transfer of funds (IBC2, 2.95±1.074), chances of providing password to fake websites (IBC3,

2.90±1.193) and sharing of account related information with third party by the bank (IBC6, 2.79±1.044). From above analysis, it may be concluded that those who are using internet banking, even their level of concern is high about various dimensions of security and privacy of internet banking. The prime reason for such concern may be attributed to increase in number of internet banking frauds.

Bank –wise, respondents' security and privacy concern regarding use of internet banking has been shown in Table 5.20.

Table 5.20
Security and Privacy Concern regarding use of Internet Banking
(Bank wise Analysis)

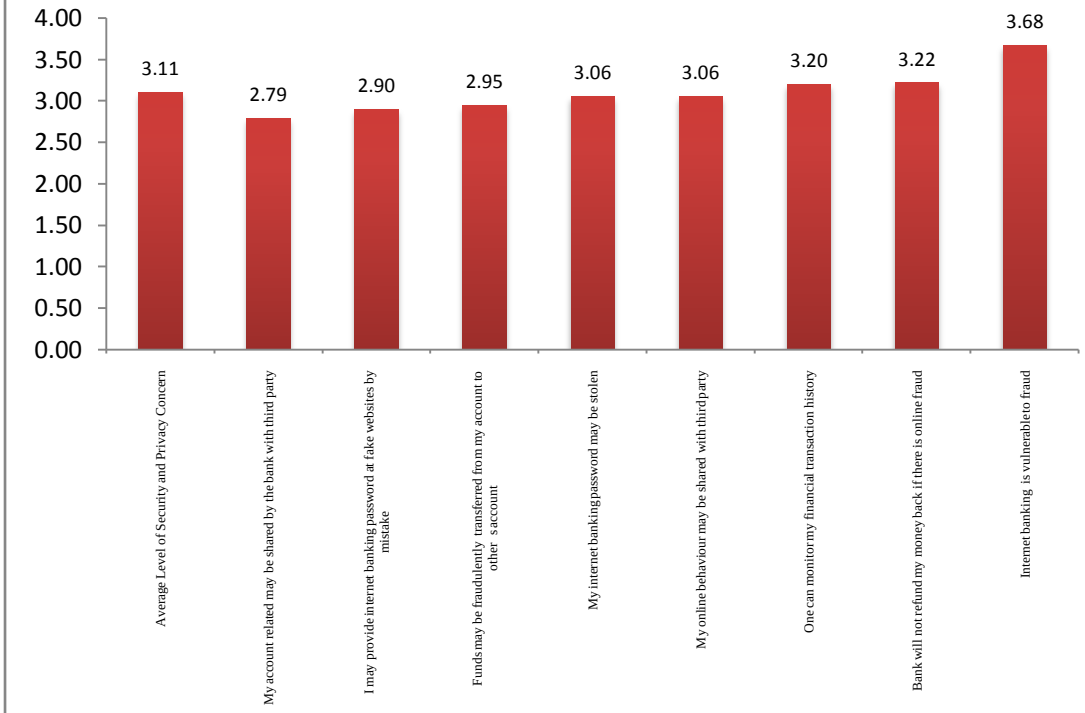
N=142

Item Code	Statement	Public Sector Banks		Private Sector Banks		ANOVA Statistic Df(3,138)	
		SBI	PNB	ICICI	HDFC	F-Value	P-value
IBC1	My internet banking password may be stolen	3.1667	3.4500	2.9286	2.8684	1.426	.238
IBC2	Funds may be fraudulently transferred from my account to other's account	3.1190	3.2500	2.7381	2.8421	1.558	.202
IBC3	I may provide internet banking password at fake websites by mistake	2.6190	3.1500	2.6190	3.3947	4.308	.006*
IBC4	One can monitor my financial transaction history	3.1429	3.7500	2.7381	3.5000	5.910	.001*
IBC5	Bank will not refund my money back if there is online fraud	3.3095	2.7500	2.9048	3.7105	6.589	.000*
IBC6	My account related may be shared by the bank with third party	2.6429	2.4500	2.4524	3.5000	9.878	.000*
IBC7	My online behaviour may be shared with third party	2.8571	2.6500	3.1667	3.3684	2.316	.078
IBC8	Internet banking is vulnerable to fraud	3.4524	3.6500	3.7143	3.8947	1.492	.219
Level of Security and Privacy Concern		3.0387	3.1375	2.9077	3.3849	3.171	.026*

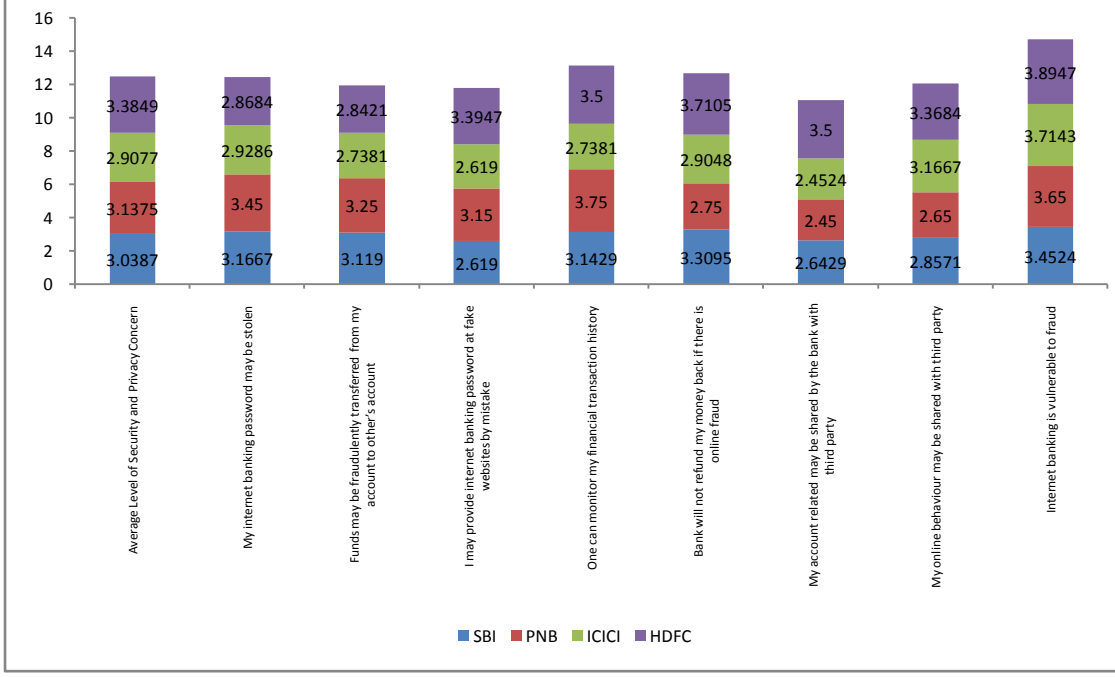
**Significant at .05*

Table 5.20 shows that overall level of security and privacy concern regarding use of internet banking was highest in among respondents of HDFC (3.3849) followed by PNB (3.1375), SBI (3.0387) and ICICI (2.9077). ANOVA test shows that there was significant difference in bank customers' perception towards security and privacy concern regarding use of Internet Banking across selected banks [F (3,138) = .3.71, p=.026]. Thus, Null hypothesis ($H_0$4) is rejected.

Figure 5.6: Level of 'Security and Privacy' concern (Internet Banking)



Figurre 5.7: Bank-wise level of 'security and privacy concern'(Internet Banking)



Further, there was significant difference in bank customers' perception towards security and privacy concern regarding use of Internet Banking across selected banks with respect to items IBC3 [F(3,138)=4.308, p=0.006], IBC4 [F(3,138)=5.910, p=0.01], IBC5 [F(3,138)=6.589, p=0.00], IBC6 [F(3,138)=9.878, p=0.00]. For rest of the items, there is no significant difference in level of security and privacy concern regarding use of internet banking across selected banks.

5.4.5 Perception toward Security and Privacy satisfaction regarding use of Internet Banking

Respondents' satisfaction level regarding security and privacy of Internet Banking has also been measured. The purpose of measuring satisfaction level regarding security and privacy was to find out the relationship between security and privacy concern and satisfaction level regarding the use of internet banking. To measure the security and privacy satisfaction level regarding use of Internet Banking , a self developed 11 items *'Security and Privacy satisfaction :Internet Banking'* construct was used. Respondents were asked to indicate their opinion about given statements on Five point Likert Scale ranging from 'Strongly Agree' to 'Strongly Disagree'. The statements on different aspects of security and privacy satisfaction were designed in such a way that agreeableness to the statement would reflect the higher satisfaction for given aspect or vice versa. Further, mean scores have been calculated for each statement by assigning weights of 5,4,3,2 and 1 to 'Strongly Agree', 'Agree', 'Neutral', 'Disagree' and 'Strongly Disagree'. The mean score of Security and Privacy satisfaction was measured by taking the Grand Mean of all the statements. Descriptive statistics and bank-wise customers' perception towards 'security and privacy satisfaction' regarding Internet Banking have been shown in Table 5.21 and Table 5.22 respectively.

Table 5.21
Descriptive of Security and Privacy satisfaction level regarding use of Internet Banking

N=142

Item Code	Statement	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	Mean± SD
IBS1	It is safe to use internet banking of my bank	0	0	37	89	16	3.8521±.59486
IBS2	The site has virtual keyboard to enter Password and User ID	1	8	20	88	25	3.9014±.77469
IBS3	The site provides security guidelines on home page	0	1	15	103	23	4.0423±.54413
IBS4	OTP(One Time Password) is required, if logging from different browsers/computers	0	8	27	78	29	3.9014±.78379
IBS5	OTP is required while making Third Party payments	0	5	35	78	24	3.8521±.73366
IBS6	OTP is always required while adding beneficiary	0	2	52	62	26	3.7887±.75165
IBS7	Pressing back space results in immediately logout from session	0	15	26	65	36	3.8592±.91939
IBS8	Idle time log out from session exists at my Bank's site	0	1	2	13	89	4.1197±.67878
IBS9	There is maximum number of incorrect password submissions	0	3	12	14	73	3.9507±.95522
IBS10	Bank provide me the facility of choosing strong password for internet banking	0	5	12	75	50	4.1972±.73648
IBS11	Bank remind me to change password from time to time	0	20	28	65	29	3.7254±.94640
Mean score of Security and Privacy Satisfaction		3.9264±.48492					

Table 5.21 shows that respondent' degree of overall security and privacy satisfaction level regarding use of internet banking was 'high' (3.9264±.48492). Statement wise, respondents' satisfaction level was 'very high' regarding facility of choosing a strong password (IBS10, 4.1972±.73648) followed by satisfaction toward Idle time log out (IBS8, 4.1197±.67878) and provision of security guidelines on home page (IBS3, 4.0423±.54413). The satisfaction level was found 'high' in case of maximum number of incorrect password submissions (IBS9, 3.9507±.95522), availability of virtual key board (IBS2, 3.9014±.77469), requirement of OTP if login from different locations (3.9014±.78379), immediate logout from session if back space button pressed (IBS7, 3.8592±.91939), safe use of Internet banking (IBS1, 3.8521±.59486), requirement of OTP for third party payments (IBS5, 3.8521±.73366), requirement of OTP to add third party (IBS6, 3.7887±.75165) and

reminder of password change (3.7254±.94640). Bank-wise, security and privacy satisfaction level regarding use of Internet Banking has been shown in Table 5.22.

Table 5.22
Security and Privacy satisfaction level regarding use of Internet Banking (Bank-wise Classification)

N=142

Item Code	Statement	Public Sector Banks		Private Sector Banks		ANOVA Statistic Df(3,138)	
		SBI	PNB	ICICI	HDFC	F-Value	P-value
IBS1	It is safe to use internet banking of my bank	3.9762	3.7500	3.9762	3.6316	3.311	.022*
IBS2	The site has virtual keyboard to enter Password and User ID	3.8810	3.4500	4.0714	3.9737	3.201	.025*
IBS3	The site provides security guidelines on home page	3.9762	4.1000	4.1190	4.0000	.632	.596
IBS4	OTP(One Time Password) is required, if logging from different browsers/computers	3.6429	3.8500	4.0238	4.0789	2.632	.053
IBS5	OTP is required while making Third Party payments	3.8571	3.2500	3.9762	4.0263	6.229	.001*
IBS6	OTP is always required while adding beneficiary	3.7381	3.6500	3.9286	3.7632	.786	.504
IBS7	Pressing back space results in immediately logout from session	4.0000	3.5500	3.9286	3.7895	1.241	.297
IBS8	Idle time log out from session exists at my Bank's site	3.9762	4.2000	4.2381	4.1053	1.155	.330
IBS9	There is maximum number of incorrect password submissions	3.7619	3.8000	4.2381	3.9211	2.036	.112
IBS10	Bank provide me the facility of choosing strong password for internet banking	4.1429	4.2000	4.2381	4.2105	.121	.947
IBS11	Bank remind me to change password from time to time	4.0000	3.6500	3.4524	3.7632	2.482	.064
Mean score of Security and Privacy Satisfaction		3.9048	3.7682	4.0173	3.9330	1.238	.298

Significant Level .05

Table 5.22 shows that degree of overall Security and Privacy satisfaction level regarding use of Internet Banking was 'very high' among respondents of ICICI (4.0173). The level of satisfaction was 'High' among respondents from HDFC (3.9330), SBI (3.9048) and PNB (3.7682). However, ANOVA test shows that there is no significant difference in bank customers' perception towards security and privacy satisfaction regarding use of Internet Banking across selected banks [F(3.138=1.238, p=.298). Thus, hypothesis H_{05} is accepted.

Figure 5.8: Level of 'Security and Privacy' satisfaction (Internet Banking)

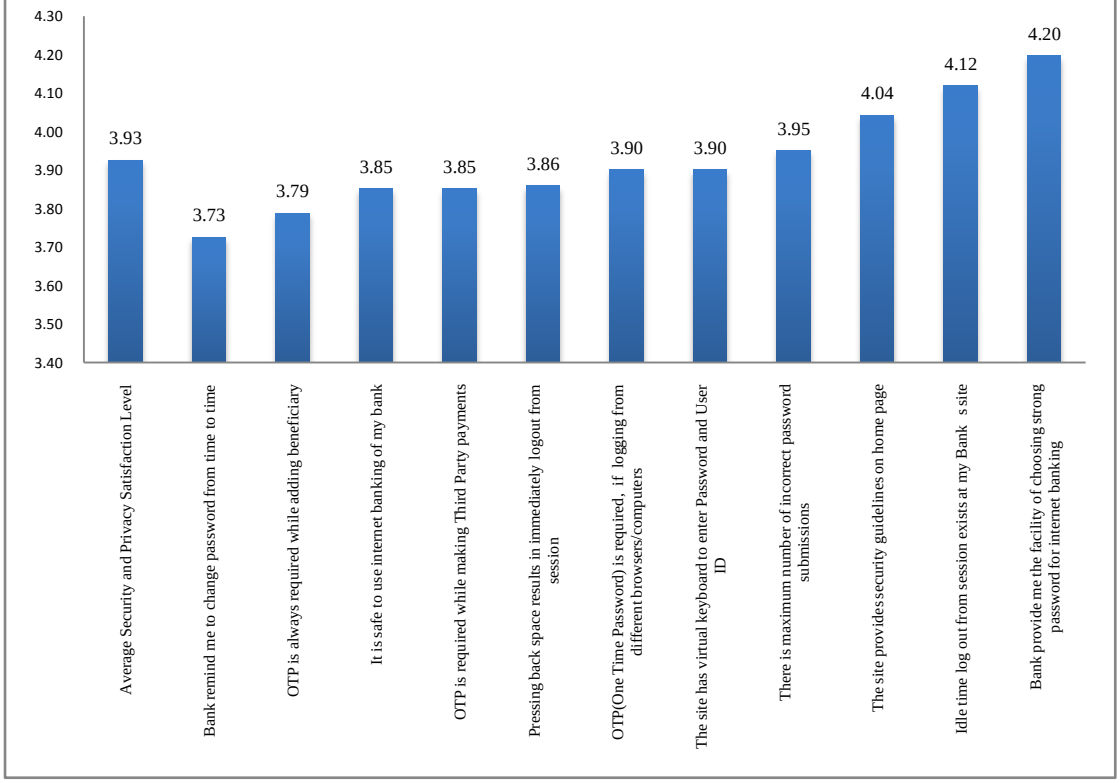
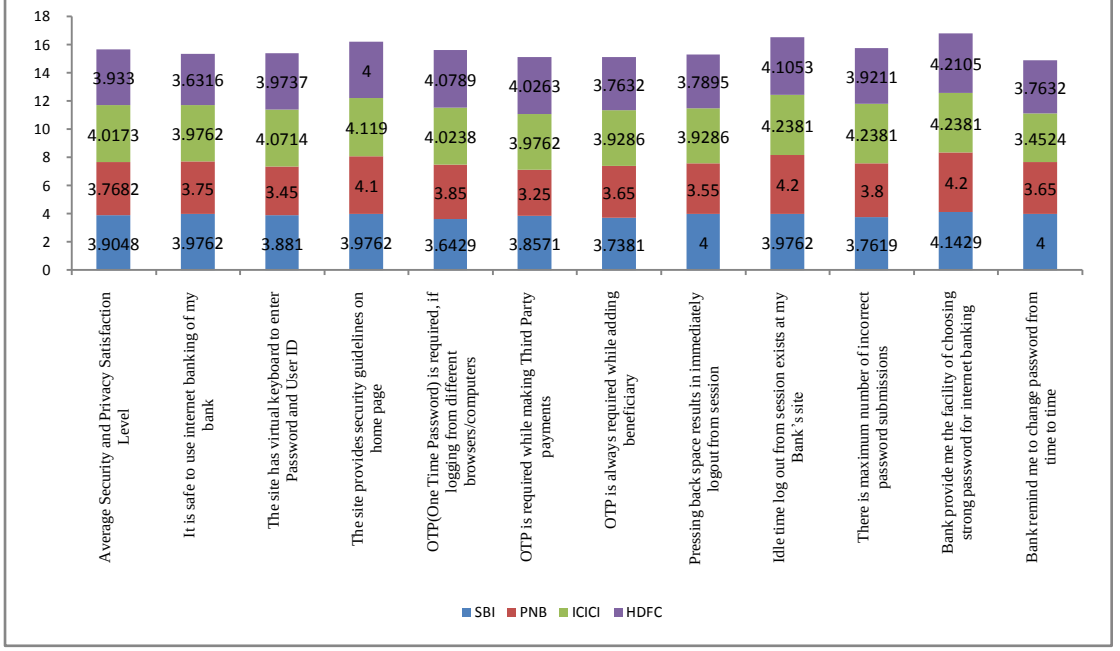


Figure 5.9: Bank-wise level of 'security and privacy' satisfaction (Internet Banking)



Analysis of each statement shows that there is significant difference in bank customers' perception towards security and privacy satisfaction regarding use of Internet Banking across selected banks with respect to items; IBS1[F(3,138) = 3.311, p =.022], IBS2[F(3,138)=3.201, p=.025] and IBS5[F(3,138)=6.229, p=.001]. For rest of the statements there is was significant difference in Security and Privacy satisfaction level regarding use of Internet Banking across selected banks.

5.4.6 Relationship between Security & Privacy Concern and satisfaction level (Internet Banking)

To establish the relationship between bank customers' perception towards 'Security & Privacy Concern' and 'Security & Privacy Satisfaction' regarding use of ATM, Pearson's coefficient of correlation was calculated (Table 5.23).

Table 5.23
Correlation between Security & Privacy Concern and Security & Privacy Satisfaction Level (Internet Banking)

Pearson Correlation	r	P
	-.300**	.000
N	142	

Significant at .01level

Table 5.23 shows that there was negative and significant correlation between Privacy Concern and Security & Privacy Satisfaction level regarding use of internet banking [r (142) = -.300, p=.000)]. Thus Null hypothesis $H_0$6 is rejected.

It is evident that with the increase in Security & Privacy Concern, the level of Security & Privacy Satisfaction will decrease in case of internet banking or vice versa.

5.5 SECURITY AND PRIVACY ISSUES REGARDING USE OF MOBILE BANKING

Mobile banking mobile banking transactions have seen some growth after its launch in India. But, Mobile banking still has a long way to go, as majority of customers prefer banking in the traditional ways (Ashta, 2010; Wang, Wang, Lin & Tang, 2003). In this context, researcher studied bank customers' perception towards

security and privacy issues regarding the use of Mobile Banking. Respondents were asked questions about Adoption and Mode of using Mobile Banking. Further respondents' perception towards concern and satisfaction level regarding use of Mobile banking has been measured.

5.5.1 Adoption and mode of using Mobile Banking

Respondents were asked about adoption and mode of using mobile banking to understand the usage behavior of them. Respondents' responses have been shown in Table 5.24 and Table 5.25.

Table 5.24
Adoption of Mobile Banking
(Bank-wise Classification)

N=190

Response	Public Sector Banks		Private Sector Banks		Total
	SBI	PNB	ICICI	HDFC	
Yes	6 (12.2)	17 (36.2)	12 (26.1)	21 (43.8)	56 (29.47)
No	43 (87.8)	30 (63.8)	34 (73.9)	27 (56.2)	134 (70.52)
Total	49	47	46	48	190

Table 5.24 shows that among surveyed respondents only 29.47 per cent of respondents were using mobile banking. Bank-wise result shows that highest number of respondents from HDFC (43.8%) was mobile banking users, followed by PNB (36.2%), ICICI (26.1%) and HDFC (12.2%).Respondents' responses regarding mode of using Mobile banking have been show in Table 5.25.

Table 5.25
Mode of Using Mobile Banking
(Bank-wise Classification)

N=56

Mode	Public Sector Banks		Private Sector Banks		Total
	SBI	PNB	ICICI	HDFC	
Through Browser	3 (50.00)	4 (23.5)	3 (25.0)	0 (0.00)	10 (17.85)
Through Mobile Banking Application	3 (50.0)	8 (47.1)	9 (52.1)	11 (52.4)	31 (55.35)
Through SMS	1 (16.7)	13 (76.5)	4 (33.3)	15 (71.4)	33 (58.92)
N	6	17	12	21	56

Table 5.25 shows that among mobile banking users, 58.92 per cent of respondents were using mobile banking through SMS followed by Mobile banking application (55.35%). Only 17.85 per cent of respondents were using mobile through browser. It seems that SMS and Mobile banking application are the preferred mode of mobile banking.

Table 5.25(1)
Mobile phone and Use of mobile Banking

N=190

Type of Mobile	Mobile Banking		Total
	Yes	No	
Classic	5 (13.9)	31 (86.1)	36
Smart	51 (33.1)	103 (66.9)	154
N	56	134	190

Table 5.25(1) shows that 33.1 percent of respondents having smart phone were using mobile banking and 13.9 percent of classic mobile users were using mobile banking.

5.5.2 Perception towards Security and privacy concern regarding use of Mobile banking

To measure the mobile banking users' perception toward 'security and privacy concern' regarding use of mobile banking, a self developed 10 items *'Security and Privacy Concern: Mobile Banking'* construct was used. Respondents were asked to indicate their opinion about given statements on Five point Likert Scale ranging from 'Strongly Agree' to 'Strongly Disagree'. The statements on different aspects of security and privacy concerns were designed in such a way that agreeableness to the statement would reflect the higher concern for given aspect or vice versa. Further, mean scores have been calculated for each statement by assigning weights of 5,4,3,2 and 1 to 'Strongly Agree', 'Agree', 'Neutral', was measured by calculation Grand Mean of all the statements. Descriptive statistics and bank-wise respondents' perception towards 'security and privacy concern' regarding mobile banking use have been shown in Table 5.26 and Table 5.27 respectively.

Table 5.26
Security and privacy concern regarding use of Mobile Banking
(Descriptive statistics)

N=56

Item Code	Statement	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	Mean± SD
MBC1	My mobile banking password may be stolen	6	15	12	18	5	3.02±1.183
MBC2	Funds may be fraudulently transferred by using mobile banking	2	21	16	14	3	2.91±.996
MBC3	I may provide mobile banking password at fake websites by mistake	1	13	15	24	3	3.27±.944
MBC4	Mobile service providers may monitor my financial transaction.	4	6	11	26	9	3.54±1.111
MBC5	It is very easy for others to 'Add payee' form my mobile banking account	1	7	34	9	5	3.18±.834
MBC6	Bank will not refund my money back if there is online fraud	0	2	37	8	9	3.43±.806
MBC7	My personal information may be shared by the bank with third party	4	12	9	24	7	3.32±1.162
MBC8	Mobile banking is vulnerable to fraud	3	8	11	28	6	3.46±1.044
MBC9	If my phone is stolen, someone else can use my mobile banking	4	5	19	25	3	3.32±.974
MBC10	My confidential mobile banking information may be accessed by others through blue tooth	6	9	29	7	5	2.93±1.042
Level of Security and Privacy Concern		3.2375 ±.67111					

Table 5.26 shows that degree of overall level of security and privacy concern regarding use of mobile banking was 'high' (3.2375±.67111). Statement-wise analysis shows that level security and privacy concern was 'high' regarding the monitoring of banking transactions by the mobile service provider (MBC4, 3.54±1.111). It was followed by the concern towards vulnerability of fraud (MBC8, 3.46±1.044), non refunding of money in case of fraud (MBC6, 3.43±.806), sharing of personal information (MBC7, 3.32±1.162), use of mobile banking by others in case mobile is stolen (3.32±.974), chances of providing of password to fake websites (MBC3, 3.27±.944), easy for others to add payee (MBC5, 3.18±.834) and stolen of password (MBC1, 3.02±1.183). The degree of concern was 'moderate' regarding transfer of confidential information through Bluetooth (MBC10, 2.93±1.042) and fraudulent transfer of funds (MBC2, 2.91±.996).

Table 5.27
Security and Privacy Concern regarding use of Mobile Banking
(Bank wise Analysis)

N=56

Item Code	Statements	Public Sector Banks		Private Sector Banks		Kruskal-Wallis Statistic Df(3)	
		SBI	PNB	ICICI	HDFC	χ^2	P-value
MBC1	My mobile banking password may be stolen	3.1667	2.5294	2.6667	3.5714	8.392	.039*
MBC2	Funds may be fraudulently transferred by using mobile banking	2.8333	2.8824	2.3333	3.2857	6.335	.096
MBC3	I may provide mobile banking password at fake websites by mistake	2.6667	3.6471	2.5833	3.5238	12.903	.005*
MBC4	Mobile service providers may monitor my financial transaction.	3.1667	3.1176	3.4167	4.0476	9.343	.025*
MBC5	It is very easy for others to 'Add payee' form my mobile banking account	3.0000	3.0588	2.8333	3.5238	7.059	.070
MBC6	Bank will not refund my money back if there is online fraud	3.3333	3.3529	3.3333	3.5714	2.042	.564
MBC7	My personal information may be shared by the bank with third party	2.8333	3.1176	2.6667	4.0000	13.860	.003*
MBC8	Mobile banking is vulnerable to fraud	3.0000	3.1176	3.2500	4.0000	11.404	.010*
MBC9	If my phone is stolen, someone else can use my mobile banking	2.8333	2.8824	3.5000	3.7143	9.191	.027*
MBC10	My confidential mobile banking information may be accessed by others through blue tooth	2.3333	2.6471	3.0000	3.2857	5.393	.145
Level of Security and Privacy Concern		2.9167	3.0353	2.9583	3.6524	5.374	.003*

Significant at .05

Table 5.27 shows that respondents' level of security and privacy concern was 'high' among respondents of HDFC (3.6524) and PNB (3.0353). On the other hand, it was found 'moderate' in case of ICICI (2.9583) and SBI (2.9167). Kruskal Wallis test shows that there was significant difference in the bank customers' perception towards security and privacy concern regarding use of Mobile Banking across selected banks. ($\chi^2(3)= 5.374$, p=.003). Therefore, null hypothesis ($H_0 7$) is rejected.

Figure 5.10: Level of 'Security and Privacy' concern (Mobile Banking)

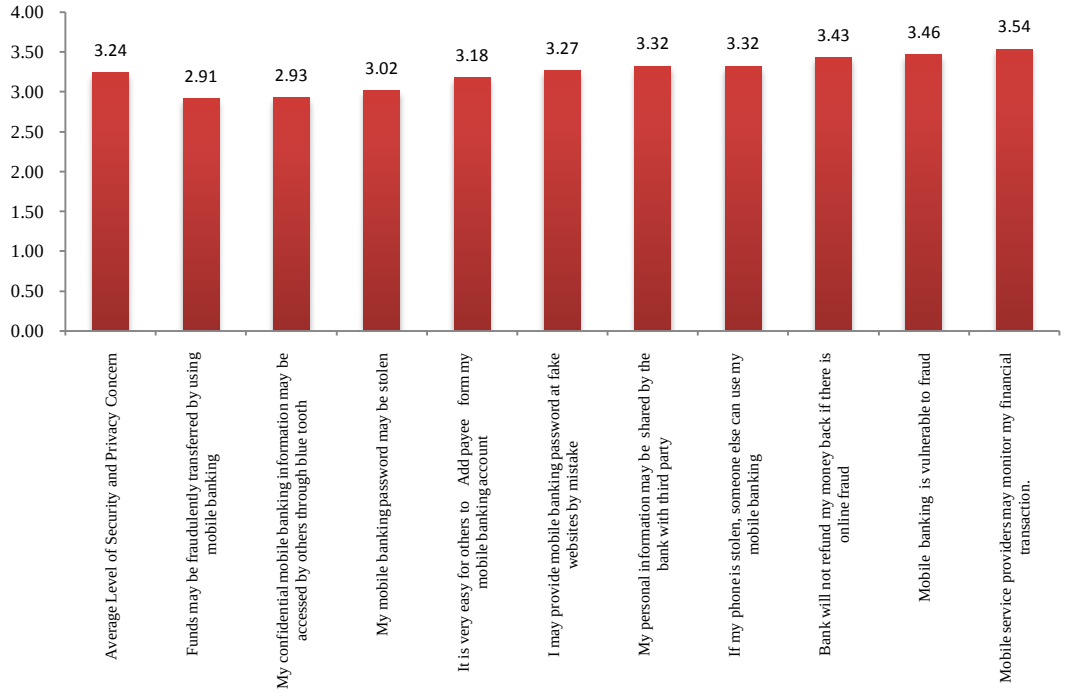
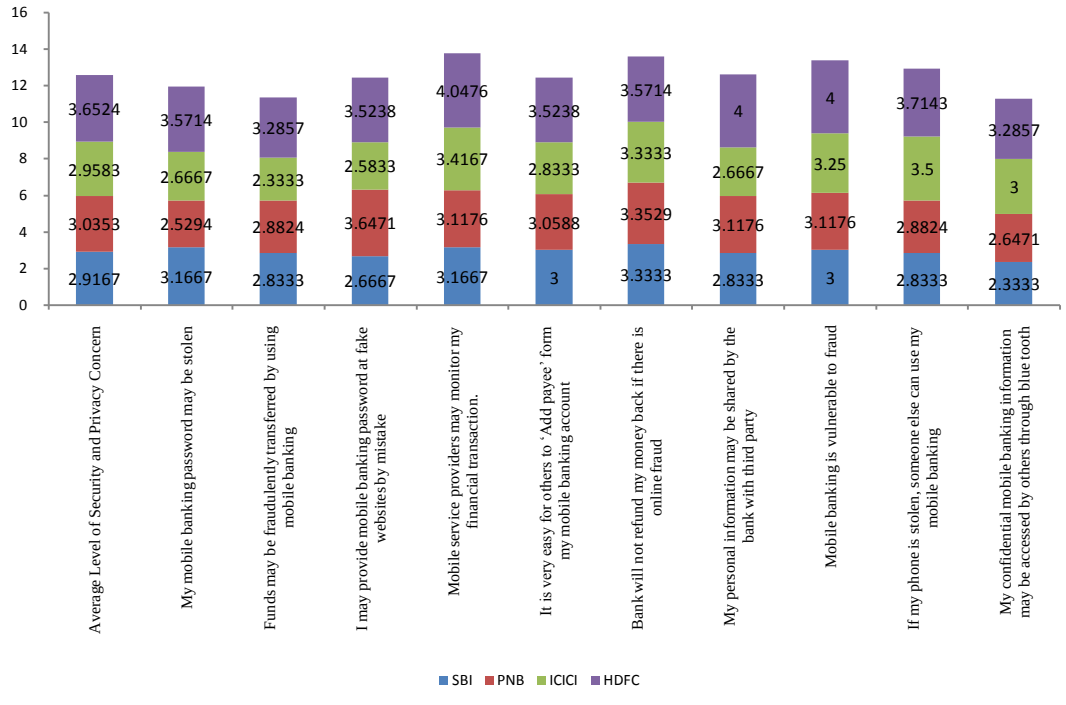


Figure 5.11: Bank-wise level of 'security and privacy concern'(Mobile Banking)



Further, analysis of each statement on different aspects of concern shows that there is significant difference in the bank customers' perception towards security and privacy concern regarding use of Mobile Banking across selected banks. with respect to itemsMBC1 ($\chi^2(3)$ =8.392, p=.039), MBC3 ($\chi^2(3)$ =12.903, .005), MBC4 ($\chi^2(3)$ =9.343, p=.025), MBC6 ($\chi^2(3)$ =8.392, p=.039), MBC7 ($\chi^2(3)$ =13.860, p=.003) and MBC8 ($\chi^2(3)$ =11.404, p=.010) and MBC9 ($\chi^2(3)$ =9.191, p=.027).

5.5.3 Perception towards Security and Privacy satisfaction regarding use of Mobile Banking

Respondents' satisfaction level regarding security and privacy of Mobile Banking has also been measured. The purpose of measuring satisfaction level regarding security and privacy was to find out the relationship between security and privacy concern and satisfaction level regarding the use of Mobile banking.

To measure the security and privacy satisfaction level regarding use of Mobile Banking , a self developed 10 items *'Security and Privacy satisfaction :Mobile Banking'* construct was used. Respondents were asked to indicate their opinion about given statements on Five point Likert Scale ranging from 'Strongly Agree' to 'Strongly Disagree'. The statements on different aspects of security and privacy satisfaction were designed in such a way that agreeableness to the statement would reflect the higher satisfaction for given aspect or vice versa. Further, mean scores have been calculated for each statement by assigning weights of 5,4,3,2 and 1 to 'Strongly Agree', 'Agree', 'Neutral', 'Disagree' and 'Strongly Disagree'. Mean score of Security and Privacy satisfaction was measured by taking the Grand Mean of all the statements. Descriptive and bank-wise security and privacy satisfaction regarding mobile Banking have been shown in Table 5.28 and Table 5.29 respectively.

Table 5.28
Satisfaction Level regarding Security and Privacy of Mobile Banking
(Descriptive Statistics)

N=56

Item Code	Statement	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	Mean± SD
MBS1	It is safe to use mobile banking of my Bank	0	2	10	36	8	3.89±.679
MBS2	Security guidelines are displayed before using Mobile banking	3	8	14	27	4	3.37±1.001
MBS3	There is maximum number of incorrect password submissions	3	0	15	29	9	3.73±.924
MBS4	My Bank provide me the facility of choosing strong password	0	0	9	36	11	4.04±.602
MBS5	OTP (One Time Password) is always required while making Third Party payments	0	2	14	31	9	3.84±.733
MBS6	OTP is always required while adding payee account on my site	0	1	29	20	6	3.55±.711
MBS7	Pressing back space results in immediately logout from session	1	1	11	30	13	3.95±.818
MBS8	Idle time log out from session exists at my Bank's site	0	1	7	37	11	4.04±.631
MBS9	My bank does not share my personal information with other sites	2	13	12	19	10	3.39±1.139
MBS10	My mobile banking site protects information about my onsite behaviour	2	12	16	20	6	3.29±1.039
Mean Score of Security and Privacy Satisfaction		3.7089 ±.43871					

Table 5.28 shows that overall Security and Privacy Satisfaction Level of respondents' regarding use of mobile banking was 'high' (3.7089 ±.43871). Statement wise analysis shows that respondents had shown very high degree of satisfaction toward facility of choosing of strong password (MBS4, 4.04±.602) and idle log out time (MBS8, 4.04±.631. The degree of satisfaction was 'high' in case of logout from session if back button is pressed (MBS7, 3.95±.818), mobile banking is safe (MBS1, 3.89±.679), Requirement of OTP (MBS5, 3.84±.733), limit of incorrect passwords (MBS3, 3.73±.924), Requirement of OTP to add payee (MBS6, 3.55±.711), sharing of personal information (MBS9, 3.39±1.139), security guidelines at home page (MBS2, 3.37±1.001) and privacy of online behavior (MBS10, 3.29±1.039).

Table 5.29
Satisfaction Level regarding Security and Privacy of Mobile Banking
(Bank-wise Analysis)

N=56

Item Code	Statement	Public Sector Banks		Private Sector Banks		Kruskal-Wallis Statistic Df(3)	
		SBI	PNB	ICICI	HDFC	χ^2	P-value
MBS1	It is safe to use mobile banking of my Bank	4.0000	4.1765	3.5833	3.8095	5.295	.151
MBS2	Security guidelines are displayed before using Mobile banking	4.0000	3.8235	3.2500	2.9048	9.751	.021*
MBS3	There is maximum number of incorrect password submissions	4.0000	3.8235	4.3333	3.2381	11.264	.010*
MBS4	My Bank provide me the facility of choosing strong password	4.1667	4.0588	3.8333	4.0952	1.763	.623
MBS5	OTP (One Time Password) is always required while making Third Party payments	3.8333	3.6471	3.9167	3.9524	2.267	.519
MBS6	OTP is always required while adding payee account on my site	3.5000	3.1765	3.9167	3.6667	9.301	.026*
MBS7	Pressing back space results in immediately logout from session	3.3333	4.0588	3.7500	4.1429	3.229	.358
MBS8	Idle time log out from session exists at my Bank's site	3.3333	4.0588	3.9167	4.2857	9.375	.025*
MBS9	My bank does not share my personal information with other sites	3.8333	3.8235	3.3333	2.9524	6.252	.100
MBS10	My mobile banking site protects information about my onsite behaviour	3.6667	3.7647	3.0000	2.9524	8.158	.043*
Security and Privacy Satisfaction Level		3.7667	3.8412	3.6833	3.6000	.994	.403

Table 5.29 shows that overall security and privacy satisfaction level regarding use of mobile banking was high among respondent of PNB (3.8412) followed by SBI (3.7667), ICICI (3.6833) and HDFC (3.6000). However, Kruskal Wallis shows that there was no significant difference in the bank customers' perception towards security and privacy satisfaction regarding use of Mobile Banking across selected banks(χ^2 (3) =.994, p=.403). Thus, null hypothesis ($H_0$8) is accepted.

Figure 5.12: Level of 'Security and Privacy' satisfaction (Mobile Banking)

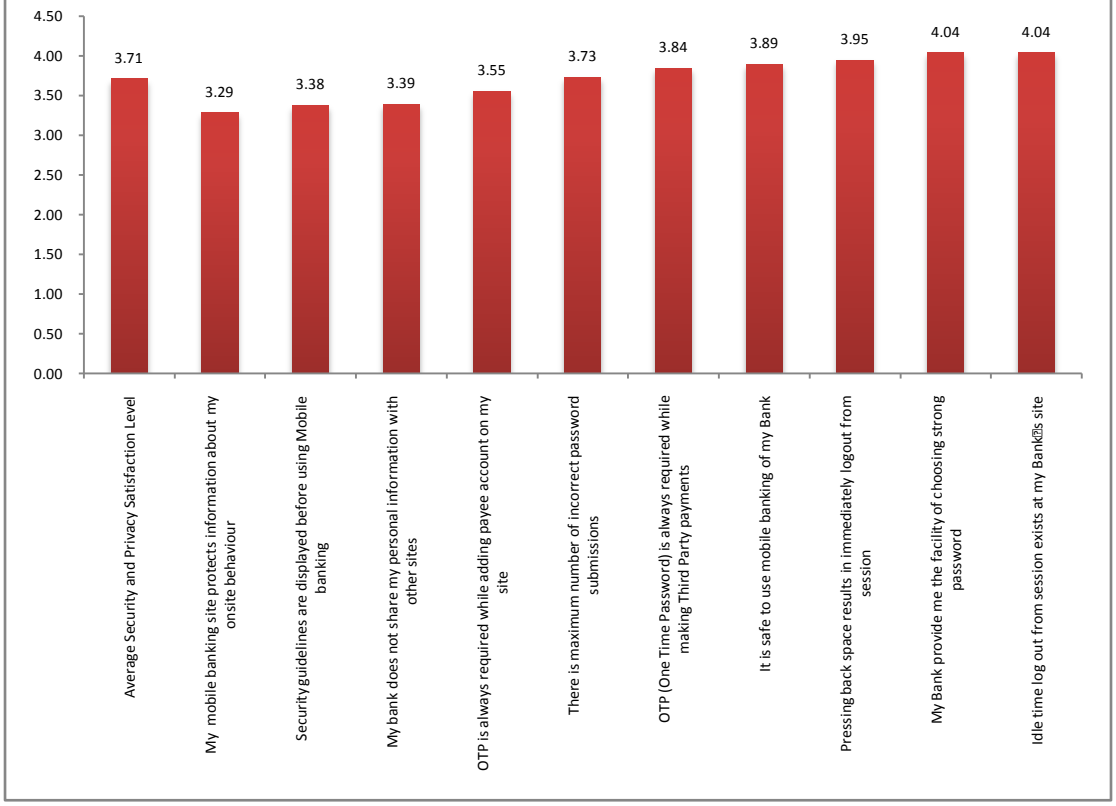
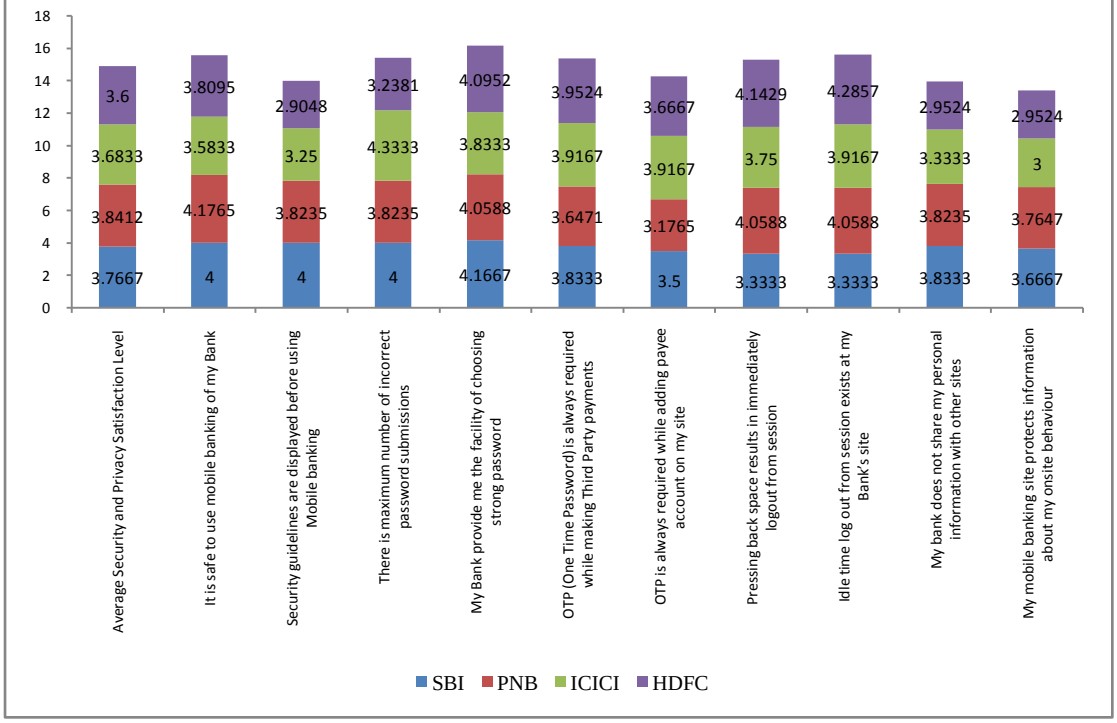


Figure 5.13: Bank-wise level of 'security and privacy' satisfaction (Mobile Banking)



Further, items wise analysis shows that there is significant difference in the bank customers' perception towards security and privacy satisfaction regarding use of Mobile Banking across selected banks with respect to items MBS2(χ^2 (3)= 9.751, p=.021), MBS3 (χ^2 (3)= 11.264,p=.010), MBS6 (χ^2 (3)= 9.301,p=.026), MBS8 (χ^2 (3)= 9.375, p=.025), MBS10 (χ^2 (3)= 8.158,p=.043).

5.5.4 Correlation between Security & Privacy Concern and Security & Privacy Satisfaction Level (Mobile Banking)

To establish the relationship between mobile banking users' perception towards 'Security & Privacy Concern' and 'Security & Privacy Satisfaction' regarding use of mobile banking, Pearson's coefficient of correlation was calculated (Table 5.30).

Table 5.30
Correlation between Security & Privacy Concern and Security & Privacy Satisfaction Level (Mobile Banking)

Pearson Correlation	**r**	**p**
	-.031	.822
N	56	

Table 5.30 shows that there is negative but insignificant correlation between mobile users' perception towards 'Security & Privacy Concern' and 'Security & Privacy Satisfaction' regarding use of mobile banking. [r (56) =-.031, p=.822)]. Therefore, Null Hypothesis ($H_0$9) is accepted.

5.6 SECURITY AND PRIVACY ISSUES REGARDING USE OF CREDIT CARDS

The security and privacy in use of credit cards has always been remained a major issue. Most of the people don't use credit cards just because of this obvious reason. Therefore, in this part of the study an attempt has been made to measure the

security and privacy concern of users regarding use of Credit cards and their satisfaction regarding security and privacy while using credit cards. Respondent were asked about questions on concern, satisfaction and mode of using credit card

5.6.1 Adoption and mode of using credit cards

Respondents' adoption and mode of using credit card has been shown in Table 5.31.

Table 5.31
Mode of using credit Card

N=71

Usage of credit card	Frequency
Only offline	10 (14.1)
Only Online	12 (16.9)
Both	49 (69.0)
N	71 (37.37)

Table 5.31 shows that 37.37 per cent of respondents were credit card users. Majority of respondents were using credit card both ways i.e. offline and online (69%). However, only 14.1 per cent and 16.9 per cent of respondents were using credit card offline only and online only respectively.

5.6.2 Level of Security and privacy concern regarding use of Credit Cards

To measure the perception of credit card users' towards 'security and privacy concern' regarding use of credit, a self developed 5 items *'Security and Privacy Concern: Credit Cards'* construct was used. Respondents were asked to indicate their opinion about given statements on Five point Likert Scale ranging from 'Strongly Agree' to 'Strongly Disagree'. The statements on different aspects of security and privacy concerns were designed in such a way that agreeableness to the statement

would reflect the higher concern for given aspect or vice versa. Further, mean scores have been calculated for each statement by assigning weights of 5,4,3,2 and 1 to 'Strongly Agree', 'Agree', 'Neutral', 'Disagree' and 'Strongly Disagree'. The mean score of security and privacy concern was measured by taking Grand Mean of all the statements. Descriptive of security and privacy concern regarding credit cards use have been shown in Table 5.32.

Table: 5.32
Security and privacy concern regarding use of Credit Card
(Descriptive statistics)

N=71

Item Code	Statement	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	Mean± SD
CCC1	My credit card information may be stolen	5	22	5	25	14	3.30±1.292
CCC2	My credit card may be used by others without having my card	6	18	10	27	10	3.24±1.224
CCC3	I may provide credit card information on fake websites	13	11	15	27	5	3.00±1.254
CCC4	CVV(password)of my card may be stolen	4	14	14	29	10	3.38±1.126
CCC5	My card usage information may be shared by bank with others	9	20	15	19	8	2.96±1.236
Mean score of Level of Security and Privacy Concern		3.1746 ±.93315					

Table 5.32 shows that respondents' level of security and privacy concern regarding use of credit cards was 'high' (3.1746 ±.93315). Statement-wise analysis shows that level of security and privacy concern was 'high' with respect to items security of CVV (CCC4, 3.38±1.126), stealing of credit card information (3.30±1.292), fraudulent use of credit card (CCC2, 3.24±1.224) and providing of credit card on fake sites (CCC3, 3.00±1.254). The degree of satisfaction was found 'moderate' regarding possibility of sharing of card information (CCC5, 2.96±1.236).

Figure 5.14: Level of 'Security and Privacy' concern (Credit Cards)

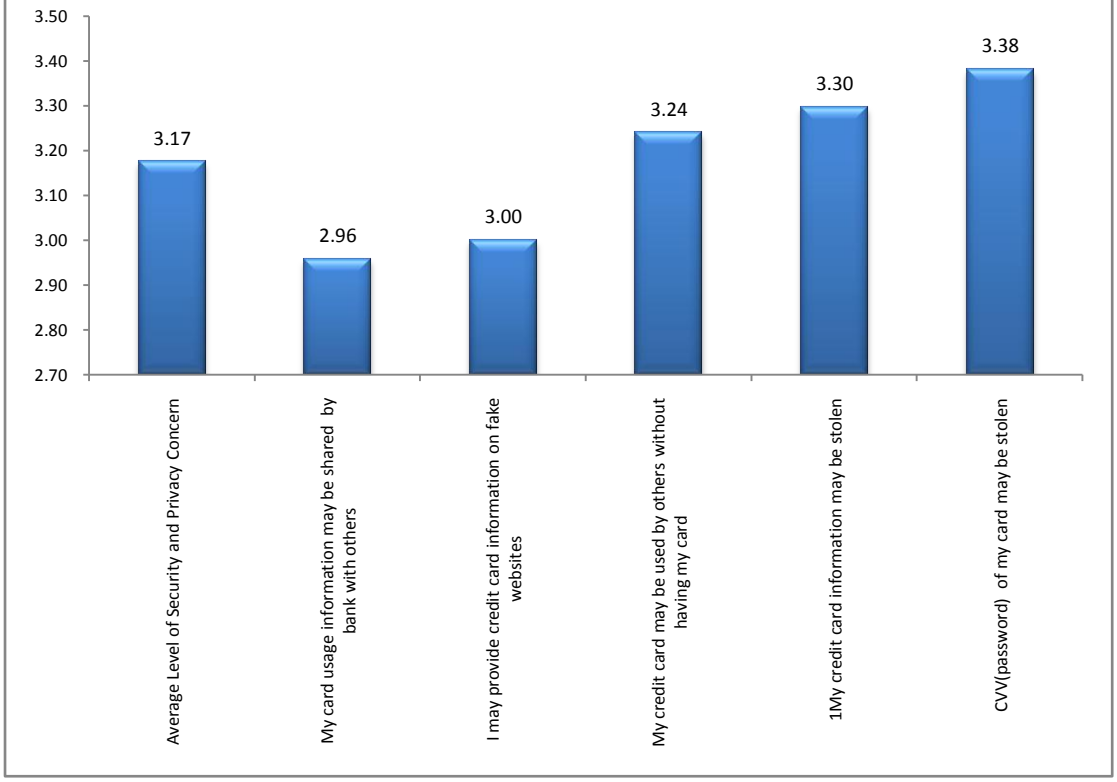
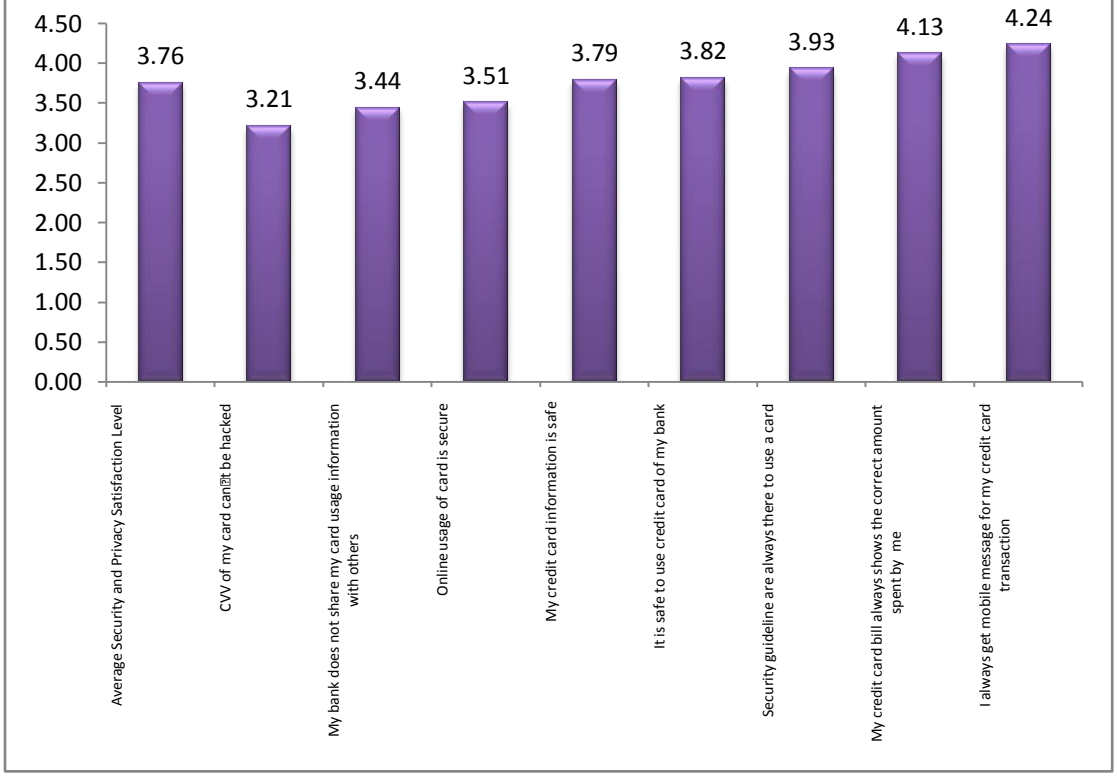


Figure 5.15: Level of 'Security and Privacy' satisfaction (Credit Cards)



5.6.3 Perception towards Security and Privacy satisfaction regarding use of Credit Cards

Respondents' satisfaction level regarding security and privacy of credit card has also been measured. The purpose of measuring satisfaction level regarding security and privacy was to find out the relationship between security and privacy concern and satisfaction level regarding the use of credit cards. To measure the security and privacy satisfaction level regarding use of credit cards, a self developed 8 items *'Security and Privacy satisfaction: Credit cards* construct was used. Respondent's satisfaction level regarding security and privacy of credit card has been shown in Table 5.33.

Table 5.33
Satisfaction Level regarding Security and Privacy of Credit Card

N=56

Item Code	Statement	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	Mean± SD
CCS1	It is safe to use credit card of my bank	2	4	8	48	9	3.82±.833
CCS2	Security guideline are always there to use a card	0	2	14	42	13	3.93±.704
CCS3	Online usage of card is secure	5	3	23	31	9	3.51±1.012
CCS4	I always get mobile message for my credit card transaction	0	1	8	35	27	4.24±.706
CCS5	CVV of my card can't be hacked	1	17	30	12	11	3.21±1.027
CCS6	My credit card bill always shows the correct amount spent by me	0	2	8	40	21	4.13±.716
CCS6	My credit card information is safe	0	5	20	31	15	3.79±.860
CCS6	My bank does not share my card usage information with others	3	7	28	22	11	3.44±1.010
Security and Privacy Satisfaction Level		3.7570 ±.54235					

Table 5.33 shows that respondents' security and privacy satisfaction level regarding use of credit cards was 'high' (3.7570 ±.54235). Statement-wise analysis shows that level of satisfaction towards receiving of mobile messages about credit card transactions (CCS4, 4.24±.706)and showing of correct amount spent in statement (CCS6, 4.13±.716) was 'very high'. On the other hand satisfaction towards security guidelines (CCS2, 3.93±.704), safe use of credit card (CCS1, 3.82±.833),

safety of credit card information (CCS6, 3.79±.860), securely online use of credit card (CCS3, 3.51±1.012), sharing of credit card information (CCS6, 3.44±1.010) and hacking of CCV (CCS5, 3.21±1.027) was found as 'high'.

5.6.4 Correlation between Security & Privacy Concern and Security & Privacy Satisfaction Level (Credit Cards)

To establish the relationship between credit card users' perception towards 'security & privacy concern' and 'security and privacy satisfaction' Pearson's coefficient of correlation was calculated (Table 5.34).

Table 5.34
Correlation between Security & Privacy Concern and Security & Privacy Satisfaction Level
(Credit Cards)

Pearson Correlation	r	p
	-.539**	**.000**
N	**71**	

Significant at .01 level

Table 5.34 shows that there is negative and significant correlation between bank customers perception toward 'Security & Privacy Concern' and 'Security & Privacy Satisfaction' regarding use of credit card [r(71) = -.539, p=.000)]. Thus, Hypothesis $H_0$10 is rejected.

It is evident that with the increase in Security & Privacy Concern, the level of Security & Privacy Satisfaction will decrease in case of credit cards or vice versa.

Section –III

5.7 OPINION OF NON-USERS OF E-BANKING SERVICES

One of the objectives of the study was to examine the opinion of non-users of e-banking services. To achieve this objective researcher conducted 20 unstructured interviews with non-users of e-banking services. The objective of interviews was limited to find out the reason(s) for not using e-banking services. E-banking channel-wise results are summarized as below.

5.7.1 Opinion of Non-Users Of ATMs

Respondents were asked to specify the reasons of not using ATMs. It was found that respondent with different demographic background articulated diffident types of reasons for not using ATMs. Following reasons were prominently figured out:

i. No need of ATM
ii. No knowledge to use ATM
iii. Happy with branch service
iv. Security and privacy risks
v. No personal touch

5.7.2 Opinion of Non-Users of Internet Banking

Respondents were asked to specify the reasons of not using internet banking. After discussion with respondents, it was found that respondents having different demographic background had different reasons for not using internet banking. Following were the main reason for not using internet banking

i. No knowledge of using internet
ii. No knowledge of using internet banking
iii. No need of internet banking
iv. Security and privacy issues
v. No internet connection at home.
vi. Lack of personal touch

5.7.3 Opinion of Non-Users of Mobile Banking

Respondents were asked to specify the reasons of not using mobile banking. Following were the main reason for not using internet banking.

i. Banking needs are fulfilled by other channel

ii. Phone is not compatible

iii. Security risk is there

iv. No knowledge of using Mobile Banking

v. No internet connection on Mobile

5.10 Opinion of Non-Users of Credit Cards

Respondents were asked to specify reasons for not using credit cards. It was found that followings were that major reasons of not using credit cards.

i. No need of credit cards

ii. Security and privacy concern.

iii. Unnecessary expenditure

iv. Debit card is sufficient.

Chapter – 6
SUMMARY, FINDINGS, CONCLUSION AND SUGGESTIONS

6.1 BACKGROUND OF THE STUDY

The evolution of e-banking has fundamentally transformed the way banks traditionally conduct their businesses and the ways consumers perform their banking activities (Eriksson et al., 2008; Sayar and Wolfe, 2007).'E-banking' has attracted the considerable amount of interest of researchers in the recent times. Majority of the studies conducted in this field, primarily, focused on the identification of factors affecting the adoption of e-Banking services i.e. ATMs, Internet Banking, Mobile banking, phone Banking, ECS, Credit/debit Cards, RTGS, NEFT etc. Review of various studies has revealed that 'reliability', 'ease of use', 'personality', 'accessibility', 'accuracy', 'security' and 'efficiency' could influence the adoption of e-banking services (Joseph et. al., 1999; Meuter et al., 2000; Yang & Jun, 2002; Joseph & Sone, 2003; Long & McMellon, 2004). However, number of studies found that concern for 'security and privacy' is the most important factor influencing the adoption of e-banking banking (Polatoglu & Kin, 2001; Devlin & Young, 2003, Srivastava, 2007).

The concern for security and privacy issues in adoption of internet banking is justifiable from the fact that according to Reserve Bank of India (RBI), in 2010-2011, Indian banks lost about Rs 2,289 Cr. in bank frauds while the loss in 2007-2008 was Rs 1,057 Cr (Jagdish Mahapatra, 2012) Similarly, according to the annual report of the Indian Computer Emergency Response Team (CERT-In), the team handled about 374 phishing incidents in 2009 ((Jagdish Mahapatra, 2012). A recent study conducted

by PwC (2012) found that data security concerns and lack of clarity on regulatory stance are two major roadblocks in the adoption of internet banking (Cloud Computing) in Indian banks. Therefore, it is evident that with electronic banking on the rise, customers are vulnerable to the risks of e-banking frauds, even as regulations are becoming more stringent as far as know your customer (KYC) rules are concerned

In this background, it is apparent that concern for 'security and privacy' is the major roadblock in the adoption of e-banking services. So, there is a need to study the security and privacy issues in depth from customers' perspective. An analysis of security features of online banking portals will help the bankers to make their online portals more secure by embedding the advanced security and privacy features in their online portals. Along with the study of online portals, the opinion of e-banking services users toward the security and privacy issues will help bankers to understand customers' concern for security and privacy while using e-banking services. Hence, the present study has been designed to study the security and privacy issues in e-banking by analyzing the contents of selected internet banking portals and the opinion of users of e-banking services.

6.2 OBJECTIVES OF THE STUDY

The specific objectives of the present study are;

1. To study the present status of e-banking services in India with respect to ATMs, Internet Banking, Mobile Banking, Credit Cards and Non-cash retail payments
2. To study the security & privacy issues and regulatory environment of e-banking services in India.
3. To examine and compare the Pre-login and Post-login security and privacy features of selected banks' online banking portals.

4. To measure and compare the level of security and privacy concern among customers of selected banks regarding the use of e-banking services.
5. To measure and compare the level of security and privacy satisfaction among customers of selected banks regarding use of e-banking services
6. To find out the relationship between security & privacy concern and security & privacy satisfaction
7. To understand the opinion of non-users of e-banking services.

6.3 HYPOTHESIS OF THE STUDY

On the basis of objectives following Null hypotheses have been framed for testing purpose**:**

$H_0$1= There is no significant difference in the bank customers' perception towards security and privacy concern regarding use of ATMs across selected banks.

$H_0$2= There is no significant difference in the bank customers' perception towards security and privacy satisfaction regarding use of ATMs across selected banks.

$H_0$3= There is no relationship between bank customers' perception of 'security &privacy concern' and 'security & privacy satisfaction' in case of ATM use.

$H_0$4= There is no significant difference in bank customers' perception towards security and privacy concern regarding use of Internet Banking across selected banks.

$H_0$5= There is no significant difference in bank customers' perception towards security and privacy satisfaction regarding use of Internet Banking across selected banks.

$H_0$6= There is no relationship between bank customers' perception of 'security &privacy concern' and 'security & privacy satisfaction' in case of Internet banking use.

$H_0$7= There is no significant difference in the bank customers' perception towards security and privacy concern regarding use of Mobile Banking across selected banks.

$H_0$8= There is no significant difference in the bank customers' perception towards security and privacy satisfaction regarding use of Mobile Banking across selected banks.

$H_0$9= There is no relationship between bank customers' perception of 'security &privacy concern' and 'security & privacy satisfaction' in case of Mobile Banking use.

$H_0$10=There is no relationship between bank customers' perception of 'security &privacy concern' and 'security & privacy satisfaction' in case of Credit Cards use.

6.4 RESEARCH METHODOLOGY

The present study has three dimensions. Firstly, it studies the security features of online banking portals where online banking portals of selected banks have been compared on the basis of security and privacy features. Secondly, it examines the perception of bank customers towards security and privacy issues in e-banking. Thirdly, it attempts to understand the view of non users of e-banking services. The theoretical scope of the study was limited to e-banking services of four banks i.e. ATM, Internet Banking, Mobile Banking and Credit cards. The geographical scope of the study was Tri-city i.e. Chandigarh UT, Mohali and Panchkula. For study purpose, four banks were selected. Selected banks were: State Bank of India (SBI), Punjab National Bank (PNB), ICICI Bank (ICICI), and HDFC Bank (HDFC).To make the comparison of security and privacy features of selected banks online portals, A Check List was prepared and used to collect the information from online portals. The check

list primarily focused on security and privacy contents of online portals. For the purpose of examining the perception of bank customers regarding security and privacy concern regarding e-banking services, a sample of 200 bank customer divided equally among selected banks was planned. However, the researcher could obtain only 190 valid questionnaires. Data was collected by using Non-Probability Judgmental sampling. A questionnaire containing eight self developed constructs was used as an instrument to collect the data. The date was analyzed using SPSS 16. Further, opinion of 20 bank customers for not using e-banking service has been studied by conducting unstructured interviews.

6.5 FINDINGS OF THE STUDY

Findings emerged from the study have been presents as under:

6.5.1 Findings based on Content analysis of Online Portals

1. HDFC Bank and ICICI Bank have provided the direct link to their online banking services from the Home page of the main website. On the other hand SBI and PNB have exclusive portal for online banking services.
2. Among selected banks, only ICICI bank has the mandatory entry of OTP if customer login from different computers or browsers. Access is granted only after entry of OTP (One Time Password) which comes in the form of SMS on registered mobile. All selected banks' online portals have virtual keyboard and Scrambled Keyboard'. However, 'Hovering Keyboard' key board and 'Scrambled Keyboard' with 'shuffle' option are present in HDFC Bank's portal only.
3. Only PNB and HDFC Bank have Multi-Factor Authentication (MFA) system for login. This feature in PNB is known as 'PNB-IBS Shield' and in HDFC

Bank as ‘Secure Access’. SBI and ICICI bank still rely on standard Authentication process i.e. User Id and password.

4. PNB, HDFC and ICICI Bank have the facility of generation of password online but in case of SBI Bank one has to visit the branch to request for new password.
5. Alert for leftover attempts in case of wrong password entry is available in case of PNB only.
6. The general practice of putting security, privacy and phishing attack information has been followed by all selected banks by putting security and privacy messages on or before the login page.
7. SBI has 256-bit Secure Socket Layer whereas rests of the selected banks have 128-bit Secure Socket Layer for encryption.
8. In case of PNB and ICICI banks user ID will expire if it is not used for more than 360 days. PNB and HDFC have made it compulsory to change the login password after specified duration. However, in case of ICICI and HDFC an alert is kept on displaying alert in this regard but it is not compulsory to change the password. The expiry period of transaction password is 180 days in case of PNB. There is no such compulsion in case of SBI.
9. All the selected banks display last login time and date on their portals.
10. In case of SBI, one needs to enter profile password for number of online transactions. However, this feature is not available in rest of the banks. They use other security methods for this purpose. In case of SBI and PNB it is compulsory to enter OTP to Add Payee. But, in case of ICICI and HDFC Debit Card Grid Authentication is required.

11. The option to assign maximum transfer limit to account is another security feature. All the selected banks have his facility in their internet banking.
12. All selected banks send mobile alert message to their customer for online transactions. With this facility, online banking users may immediately notice any unauthorized transaction.
13. PNB, HDFC and ICICI banks offer the facility of generation of password online but in case of SBI Bank one has to visit the branch to request for new password. From convenience point of view online generation of password is very good feature but there might be security concerns in this regard.
14. All selected banks' online portals have 'Idle Time log out' and all the selected banks have 'Backspace' 'Fresh' 'Forward' logout feature.

6.5.2 Findings based on bank customers' perception toward security and privacy issues in e-banking

1. Age-wise distribution of respondents showed that majority of the respondents (61.6%) were from age groups 'Less than 25' (31.1%) and '25-35' (30.5%) taken together. It was followed by age groups '35-45' (24.7%), '45-55' (12.1%) and 'Above 55' (3.2%). Thus, study found that e-banking services were more popular among youngsters when compared with upper age groups.
2. Results of the study indicated that respondents' awareness regarding innovative banking channels i.e. 'ATM' and 'Internet Banking' was very high as all the respondents in case of ATM and 88.4 per cent of respondents in case of Internet Banking were aware of these channels. Awareness of Mobile Banking was quite good among respondents as 56.8 per cent of respondents were aware about it. The only e-banking channel about which respondents were least aware was phone banking where only 44.2 per cent of respondents

were aware of it. Bank-wise similar trend has been observed except PNB's Mobile Banking where only 40.4 per cent respondents were aware of it.

3. Majority of respondents have been using ATM for more than 4 years (68.5%). it shows that respondents had good exposure of using ATMs. It was found that customers have been using ATM very frequently to conduct the banking transaction as maximum number of respondents had been using ATM 'Once in a Fortnight' (30.0%) followed by 'Once in a week' (28.9%), and 'More than once in a week' (26.8%). Only 11.6 per cent and 2.6 per cent of respondents were using ATM 'once in a month' and 'once in a quarter' respectively.
4. The overall level of security and privacy concern regarding use of ATM showed that respondents were moderately concerned about ATM's security and privacy (2.7275±.75701). However, respondents had shown high concern about possibility of cloning of their ATM cards (ATMC1,3.15±1.16) and chances that others can see their ATM password (PIN) while entering it (ATMC8, 3.15±1.217). Moderate level of concern was shown about jamming of ATM card (ATMC9, 2.73±1.190), deduction in balance without transaction (ATMC6, 2.68±1.073) and sharing of card information by the bank with others (ATMC7, 2.66±1.245). Further, respondents had shown low level of concern towards dispensing of less amount from ATM (ATMC3, 2.39±1.176), withdrawal of amount without using card (ATMC4, 2.39±1.087) and transfer of cash from ATM without using card (ATMC5, 2.42±1.064).
5. Bank-wise, study found that overall level of security and privacy concern regarding use of ATM is highest among respondents of HDFC Bank (3.0718) followed by respondents from SBI (2.8662). Respondents from ICICI (2.5942) and PNB (2.3617) had shown moderate and very low level concern regarding

use of ATM respectively. ANOVA result shows that there was significant difference in the bank customers' perception towards security and privacy concern regarding use of ATMs across selected banks [F (3,186) = 9.006, p=0.00]. Null hypothesis $H_0$1 is rejected.

6. It was found that respondents' overall satisfaction level of ATMs' security and privacy was high (3.2063±0.4842). Among different aspects of security and privacy depicted through statements, the satisfaction level was very high regarding safety of withdrawal of cash from ATM (ATMS1, 4.03±.599) .The level was high in case of limit of maximum number of incorrect password submissions (ATMS6, 3.88±.788), availability of contact information to block ATM card (ATMS7, 3.57±.978), guidance about safety tips (ATMS5, 3.15±1.039), Safety of PIN (ATMS2, 3.07±.954), entry of one person in ATM cabin (ATM10, 3.00±1.251). Moderate level of satisfaction was found in case of privacy of password (ATMS3, 2.95±.930), privacy while using ATM (ATMS9, 2.93±1.113), Cloning of ATM card (ATMS4, 2.83±.994), and secure access of ATM doors (ATMS8, 2.65±1.258).
7. Bank- wise, study found that respondents' security and privacy satisfaction level regarding use of ATM was highest in case of PNB(3.3213), followed by SBI (3.2510), ICICI (3.1739) and HDFC (3.0792). However, One way ANOVA test shows that there was no significant difference in the bank customers' perception towards 'security and privacy satisfaction' regarding use of ATMs across selected banks [F (3,186) =2.237, p=.085]. Thus, Null hypothesis $H_0$2 is accepted.

8. Study found that there is a negative and significant correlation between & Privacy Concern and Security & Privacy Satisfaction level regarding use of ATM [r (190) = -.175, p=.016)]. However, degree of correlation was very low.
9. Study found that 74.7 per cent were using internet banking. Bank wise classification shows that maximum number of respondents from ICICI (91.3%) was Internet Banking users. It was followed by respondents from HDFC (79.2%), SBI (85.7%) and PNB (42.6%). The study reveals that respondents were using internet banking frequently to conduct banking transactions as maximum number of respondents had been using Internet banking 'once in a month' (37.3%) followed by 'Once in Fortnight' (23.9%), Once in a week (14.8%), More than one in a week'(13.4%), and 'Once in a Quarter'(10.6%)
10. Study found that 72.55 per cent of respondents were using Internet Banking for online shopping, which is highest among given options. It was followed by 'Checking of Balance' (66.90%), 'Checking of Mini Statement' (63.38%), Payment of Bills (63.38%) and 'Transfer of Funds' (61.27%). Bank-wise analysis showed that maximum proportion of respondents from HDFC (92.9%) use internet banking for online shopping followed by ICICI (78.6%), PNB (60%) and SBI (54.8%). Further, 78.7 per cent of respondents from ICICI bank use internet banking for 'Payment of Bill' followed by PNB (60.0%), SBI (54.8%), and HDFC (47.4%).
11. Majority of respondents were of opinion that they were using strong internet banking password. Further respondents were quite aware about internet banking security features as majority of respondents were aware of 'Virtual Keyboard' (88.02%) and 'One time password' (83.80%). Similarly, majority

of respondents were aware of 'Profile password' (51.40%) and Hyper Text Transfer Protocol secured (50.70%).

12. It was found that despite of the importance of virtual key board, the use of was is not very encouraging as only 16.0 per cent of respondents used virtual key board 'Always' and only 12.0 per cent used it 'Frequently'. 43.2 percent of respondents used it 'Sometimes' and 28.6 percent of respondents never used it. The proportion of virtual key board users was highest in case of SBI who use it frequently (21.9%). It was further found that only 43.2 percent of respondents and 33.6 per cent of respondents were aware of new types of virtual keyboards i.e.' Scrambled Virtual Key Board' and 'Hovering Virtual Key Board' respectively
13. With respect to security and privacy concern regarding use of internet banking it was found that, in general, respondents' level of security and privacy concern regarding use of internet banking was 'high' (3.1065 ±.72780). Statement wise analysis showed that respondents had 'high' concern with respect to vulnerability of fraud in Internet (IBC8, 3.68±0.949), password hacking (IBC1, 3.06±1.153), sharing of online behavior with third party (IBC, 3.06±1.166), non refund of money in case of fraud (IBC5, 3.22±1.011), monitoring of financial transaction history (IBC4, 3.20±1.075)
14. Bank wise study found that overall level of security and privacy concern regarding use of internet banking was high among respondents of HDFC (3.3849), PNB (3.1375) and SBI (3.0387). It was found 'moderate' in case of ICICI Bank (2.9077). ANOVA test shows that there was significant difference in bank customers' perception towards security and privacy concern regarding

use of Internet Banking across selected banks [F (3,138) = .3.71, p=.026]. Null hypothesis ($H_0$4) is rejected.

15. Study found that respondents'' degree of overall security and privacy satisfaction level regarding use of internet banking was 'high' (3.9264±.48492). Statement wise, respondents' satisfaction level was 'very high' regarding facility of choosing a strong password (IBS10, 4.1972±.73648) followed by satisfaction toward Idle time log out (IBS8, 4.1197±.67878) and provision of security guidelines on home page (IBS3, 4.0423±.54413). The satisfaction level was found 'high' in case of maximum number of incorrect password submissions (IBS9, 3.9507±.95522), availability of virtual key board (IBS2, 3.9014±.77469), requirement of OTP, if login from different locations (3.9014±.78379), immediately logout from session if back space button pressed(IBS7, 3.8592±.91939), safe use of Internet banking (IBS1, 3.8521±.59486), requirement of OTP for third party payments (IBS5, 3.8521±.73366), requirement of OTP to add third party (IBS6, 3.7887±.75165) and reminder of password change (3.7254±.94640).
16. Bank –wise overall Security and Privacy satisfaction level regarding use of Internet Banking was 'very high' among respondents of ICICI (4.0173). The level of satisfaction was 'High' among respondents from HDFC (3.9330), SBI (3.9048) and PNB (3.7682). However, ANOVA test shows that there was no significant difference in bank customers' perception towards security and privacy satisfaction regarding use of Internet Banking across selected banks [F(3.138=1.238, p=.298). Hypothesis H_{05} is accepted.

17. There was negative and significant correlation between Privacy Concern and Security & Privacy Satisfaction level regarding use of internet banking [r (142) = -.300, p=.000)]. Null hypothesis $H_0$6 is rejected.
18. The adoption rate for mobile banking was very low among the respondents as only 29.47 per cent of respondents were using mobile banking. Bank-wise results showed that highest number of respondents from HDFC (43.8%) were mobile banking users, followed by PNB (36.2%), ICICI (26.1%) and HDFC (12.2%). SMS (58.92%) and Mobile banking application (55.35%) were the preferred mode of using mobile banking.
19. Study found that the degree of overall level of security and privacy concern regarding use of mobile banking was 'high' (3.2375±.67111). Statement-wise analysis shows that level security and privacy concern was 'high' regarding the monitoring of banking transactions by the mobile service provider (MBC4, 3.54±1.111), vulnerability to fraud (MBC8, 3.46±1.044), non refunding of money in case of fraud (MBC6, 3.43±.806), sharing of personal information (MBC7, 3.32±1.162), use of mobile banking by others in case mobile is stolen (3.32±.974), chances of providing password to fake websites (MBC3, 3.27±.944), easy for others to add payee (MBC5, 3.18±.834) and stealing of password (MBC1, 3.02±1.183). The degree of concern was 'moderate' regarding transfer of confidential information through Bluetooth (MBC10, 2.93±1.042) and fraudulent transfer of funds (MBC2, 2.91±.996).
20. The level of security and privacy concern regarding use of mobile banking was found 'high' among respondents of HDFC (3.6524) and PNB (3.0353). On the other hand, it was 'moderate' in case of ICICI Bank (2.9583) and SBI (2.9167). Kruskal Wallis test shows that there was significant difference in the

bank customers' perception towards security and privacy concern regarding use of Mobile Banking across selected banks. ($\chi^2(3)= 5.374$, p=.003). Therefore, null hypothesis ($H_0$7) is rejected

21. Regarding security and privacy satisfaction level of mobile banking, it was found that degree of satisfaction was high (3.7089 ±.43871).Statement wise analysis shows that respondents had shown very high degree of satisfaction toward facility of choosing of strong password (MBS4, 4.04±.602) and idle log out time (MBS8, 4.04±.631. The degree of satisfaction was 'high' in case of logout from session if back button is pressed (MBS7, 3.95±.818), mobile banking is safe (MBS1, 3.89±.679), Requirement of OTP (MBS5, 3.84±.733), limit of incorrect passwords (MBS3, 3.73±.924), Requirement of OTP to add payee (MBS6, 3.55±.711), sharing of personal information (MBS9, 3.39±1.139), security guidelines at home page (MBS2, 3.37±1.001) and privacy of online behavior (MBS10, 3.29±1.039).
22. Bank-wise, degree of overall security and privacy satisfaction level regarding use of mobile banking was 'high' among respondent of PNB (3.8412) followed by SBI (3.7667), ICICI (3.6833) and HDFC (3.6000).However, Kruskal Wallis test results shows that there was no significant difference in the bank customers' perception towards security and privacy satisfaction regarding use of Mobile Banking across selected banks (χ^2 (3) =.994, p=.403). Thus, null hypothesis ($H_0$8) is accepted.
23. Study found that there is negative but insignificant correlation between mobile users' perception towards 'Security & Privacy Concern' and 'Security & Privacy Satisfaction' regarding use of mobile banking. [r (56) =-.031, p=.822)]. Therefore, Null Hypothesis ($H_0$9) is accepted.

24. It was found that adoption level of credit card was low as only 37.37 per cent of respondents were credit card users. The usage mode revealed that majority of respondents were using credit card both ways i.e. offline on online (69%).
25. It was found that respondents' level of concern was 'high' (3.1746 ±.93315). Statement-wise analysis shows that level of concern was 'high' regarding security of CVV (CCC4, 3.38±1.126), stealing of credit card information (3.30±1.292), fraudulent use of credit card (CCC2, 3.24±1.224) and providing credit card information (CCC3, 3.00±1.254). The degree of satisfaction was found 'moderate' regarding sharing of card information (CCC5, 2.96±1.236).
26. The overall security and privacy satisfaction level regarding use of credit cards was found 'high' (3.7570 ±.54235). Statement-wise analysis showed that level of satisfaction towards receiving of mobile messages about credit card transactions (CCS4, 4.24±.706) and showing of correct amount spent in statement (CCS6, 4.13±.716) was 'very high'. On the other hand, satisfaction towards security guidelines (CCS2, 3.93±.704), safe use of credit card (CCS1, 3.82±.833), safety of credit card information (CCS6, 3.79±.860), secured online use of credit card (CCS3, 3.51±1.012), sharing of credit card information (CCS6, 3.44±1.010) and hacking of CCV (CCS5, 3.21±1.027) was found as 'high'.
27. Study found that there was negative and significant correlation between Security & Privacy Concern and Security & Privacy Satisfaction level regarding use of credit card [r (71) = -.539, p=.000)].

6.5.3 Findings based on the opinion of non users of e-banking services

1. The opinion of non users of e-banking services revealed that majority of the respondents interviews revealed that 'no need', security and privacy risk', 'no

knowledge about operation', 'lack of personal touch', 'device compatibility' and non availability of internet' were the major reason for not using e-banking services.

6.6 IMPLICATIONS AND CONCLUSION

At present Indian banks are investing huge amount in the infrastructure to host internet banking activities. However, adoption rate of e-banking services is very low in India as compared to developed countries. Various research studies showed that apart from other factors 'concern for securities and privacy' is most important factor influencing the adoption of internet banking. The present study also found that except ATM, the level of concern for security and privacy regarding use of e-banking services is high. In this context, the findings of the study have implications for banking industry in two ways. Firstly, the comparison of security and privacy features will help the bankers to make their online portal more secure by incorporating the security features which other banks are using. Secondly, the study will be helpful to the bankers to understand the behavior of internet banking users and behaviour of non-internet banking users. It will help bankers to understand the security and privacy aspect of various e-banking services where customers have high level of concern. It will assist the bankers to retain the existing bank customer and to convert the potential users to actual e- banking users.

6.7 SUGGESTIONS TO BANKING INDUSTRY

1. When an internet banking user wants to login to internet banking portals, he uses two approaches; either typing URL in the address bar of the browser or typing key words in the search engines. In both the approaches there is a risk of web-spoofing. If someone misspells URL, it may lead him to fake website

similar to original website (Typo-squatting). On the other hand, if someone searches for his bank's online portal using search engines, search results may mislead him to fall in the trap of fake websites. Thus, it is always suggested that one should visit the online banking portal from the link provided at main 'Home Page' of the bank's site. Therefore, it is suggested that all the banks should provide link to their online portals from main Home Page rather than exclusive domain name for their online portals. Further, banks should guide their customers to follow this approach.

2. We often use internet banking portals from different locations (Computers or Browsers). If our User ID and password is known to another person, he can also use it to access our online portal from anywhere without our knowledge. During the study, researcher came across very good security feature of one of the selected bank i.e. Mandatory entry of OTP (One time password) in case access to the portal is requested from different location. Access is granted only after entry of OTP (One Time Password) which comes in the form of SMS on registered mobile. Thus, without registered mobile phone, it is impossible for others to login to online portal even if they have valid user ID and password. Therefore, it is suggested that all banks (specialty SBI, PNB and HDFC) should integrate this security feature in their online security portfolio to avoid unauthorized access to online portals.
3. Multi-Factor Authentication (MFA) strengthens security at login by using an additional form of authentication beyond the standard username and password. The solution is designed to preserve the convenience and usability of online banking while providing additional security for customers. In the process, at the time of entering password, a customer is shown an image and

text that have been personalized by him during registration. After recognizing the image, customer is sure that he going to enter the password at genuine site. It prevents the phishing attacks up to great extent. Therefore, it is suggested that every bank adopt Multi-Factor Authentication (MFA) system rather than using standard username and password.

4. Virtual key board is very good application to secure the online portals from key-loggers. All banks' online portals now have virtual keyboard. But the study found that two new types of virtual keyboard i.e. 'Scrambled key board with Shuffle option' and 'Hovering Key board' are being used by one of the bank under study. The use of these new virtual key board options showed that additional security has been provided for authentication. Thus, it is suggested that other banks should incorporate these additional options in their existing virtual keyboards. From analysis of primary data, it was found that majority of respondents were aware of virtual key board, however, very few of them were using it frequently. It is further suggested that the use of virtual key board be made compulsory for login to banking portals.
5. There seems to be risk in generating the internet banking password online. In researcher's opinion if user forget password, it should be issued offline only after proper verification of the user. This practice will leave no scope for the hackers to generate the password online.
6. Encryption plays vital role in online security. All banks should now upgrade their online portal to 256-bit Secure Socket Layer from 128-bit Security Socket Layer. SBI has already upgraded its online portal to 256-bit SSL.
7. Users hardly change internet banking password unless forced to so. But the use of same password for longer duration is not free from risk. Study found

that only in few banks it is mandatory to change the login password as well as transaction password after specified duration. It makes online banking more secure. Therefore, it is suggested that banks should make it compulsory to change the login password and transaction password after a specified duration.

8. Online banks generally send mobile alerts for banking transactions. But in few of the banks there is threshold limit, below which user will not receive mobile alert. In case of any transfer below this amount, user will not receive the mobile alert. It is suggested that there should not be any threshold limit for mobile alerts.
9. Findings of the study revealed that customers are quite aware of Internet Banking but the adoption rate is not so high. 'No need of Internet Banking', and ' no knowledge of using internet banking ' and 'Security and privacy concerns' are the main reason for non adoption of internet banking. In this context it is suggested, firstly, bank should prominently highlight the convenience of using internet banking by making customers aware of benefits of using internet banking. Bankers should make the customers aware of their internet banking needs. So that customers identify the need of using internet banking. Secondly, bank should educate the customers about how to use internet banking.
10. The level of security and privacy concern regarding use of internet banking is found high. Keeping this thing in mind banks should strive to reduce the level of concern regarding use of internet banking. Besides other medium of communication bank can use their website to disseminate the information regarding safe use of internet banking.

11. On the basis of interview with non-users of internet banking it was concluded that majority of educated people don't use internet banking because of security concerns. So there is need to build the trust. Trust can be build by making internet banking security features more stringent and reducing the number of cyber frauds on one side and making the customers aware of high standard security features on the other side.
12. On an average, customers are moderately concerned about using ATM. However, their level of concern is high about cloning of ATM card and knowing about password by others while entering it. Cloning of cards takes place only if fraudster secures information about the card by using skimming technique. Thus, bank should educate the customers about ways to avoid skimming by holding educational sessions of customers and transmitting security tips in mass media. Internet and mobile should widely be used for this purpose. Bank should use biometric[21] ATM machines to prevent the hacking of password and these can be used even by an illiterate person.
13. It is established that there is negative correlation between bank customers' perception of 'security & privacy concern' and 'security & privacy satisfaction' in case of ATM use. It clearly establishes that lesser the concern more the satisfaction. Thus, banks should always strive to reduce the level of security and privacy concern regarding use of ATMs.
14. It is found that bank customers are not very much aware of mobile banking and adoption rate is low. Keeping in mind the huge potential of mobile baking in India, it is suggested that bank should focus on mobile banking awareness. Bank should use newspapers, television, radio, internet and

[21] Biometric ATM's are the latest inventions to avoid fraud and duplication. Usually the PIN for biometric ATM's is the finger print of the card holder or his eye retina scan or face recognition, etc.

mobile to make the customers aware about usefulness of mobile banking. Proper security and privacy be provided to mobile banking users because that is the main reason for not adopting this technology. Further , banks should pay special attention to the security aspects where respondents have shown high level of concern

15. Study found that adoption rate of credit card usage is low and security and privacy concern is high. This it is suggested that bank should encourage the bank customers to use credit cards and special attention should be paid to the security aspects where respondents have shown high level of concern. Further, bank should educate customers about security tips of credit card usage such as use of CVV, use of genuine site (https) for online shopping through credit card etc.

BIBLIOGRAPHY

Books, Journals, Reports, Newspapers

Abu, Shanab E. and Pearson J.M. (2007), 'Internet banking in Jordan: The unified theory of acceptance and use of technology (UTAUT) perspective, Journal of Systems and Information Technology, Vol. 9 No. 1, pp. 78-97.

Akturan, Ulun and Tezcan, Nuray (2012), 'Mobile banking adoption of the youth market: Perceptions and intentions', Marketing Intelligence & Planning, Vol. 30 No. 4, pp. 444-459.

Alam, Syed Shah, Khatibi Ali, Santhapparaj A. Solucis and Talha Mohammad (2007), 'Development and prospects of internet banking in Bangladesh', Competitive Review: An International Business Journal, Vol. 17 No. 1/2, pp. 56-66.

Albesa, Jaume Gené. "Interaction channel choice in a multichannel environment, an empirical study." International journal of bank marketing 25.7 (2007): 490-506.

Amato-McCoy, D. (2005) 'Creating virtual value', Bank Systems and Technology, 1(22).

Amin Hanudin (2008), 'Factors affecting the intentions of customers in Malaysia to use mobile phone credit cards', Management Research News, Vol. 31 No. 7, pp. 493-503.

Baraghani, Sara Naimi. (2007). Factors Influencing the Adoption of Internet Banking, Master's Thesis, Lulea University of Technology.

Bauer Hans H., Hammerschmidt, Maik and Falk, Tomas (2005), 'Measuring the quality of e-banking portals', International Journal of Bank Marketing, Vol. 23 No. 2, pp. 153-175.

Bhatla,Tej Paul, Prabhu,Vikram and DuaAmit 92003) 'Understanding Credit Card Frauds' report available at http://www.popcenter.org/problems/credit_card_fraud/PDFs/Bhatla.pdf.

Boon ONGHway and Yu MingCheng (2003), 'Success factors in e-channel: the Malaysian banking scenario' International Journal of Bank Marketing, Vol.21 No.6/7, pp.369-377.

Celik, Hakan (2008), 'What determines Turkish customers' acceptance of internet banking?', International Journal of Bank Marketing, Vol. 26 No. 5, pp. 353-370.

Chong Alain Yee-Loong, OoiKeng-Boon, Lin Binshan and Tan Boon-I(2010), 'Online banking adoption: an empirical analysis', International Journal of Bank Marketing, Vol. 28 No. 4, 2010, pp. 267-287.

Chou, D.; and Chou, A.Y. (2000), A Guide to the Internet Revolution in Banking, Information Systems Management, Vol. 17, No. 2, pp. 51 - 57.

Danial, E.(1999), Provision of electronic Banking in UK and the republic of Ireland, International Journal of Bank Marketing, Vol.17 No. 2, pp. 72-82.

Davis, F. D. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. MIS Quarterly, 13, pp.319-340.

Dibold, 'White paper ATM fraud and security' available at http://www.diebold.com/Diebold%20Asset%20Library/dbd_atmfraudandsecurity_whitepaper.pdf.

Diniz, E., (1998), "Web banking in USA", Journal of Internet Banking and Commerce, Vol.3, No.2, e journal, accessed through www.arraydev.comon 010th September, 2012.

Elliot, S. and Loebbecke, C. 2000. 'Interactive, inter-organisational innovations in electronic commerce', Information Technology and People, 13(1): 46-66.

Eriksson, K., Kerem, K., & Nilsson, D. (2008) 'The adoption of commercial innovations in the former Central and Eastern European markets. The case of internet banking in Estonia', International Journal of Bank Marketing, 26 (3), 154-69.

Flavian, Carlos and Guinaliu, Miguel (2006), 'How bricks-and-mortar attributes affect online banking adoption', International Journal of Bank Marketing, Vol. 24 No. 6, 2006, pp. 406-423.

Garbarino, E., &. Strahilevitz, M. (2004) 'Gender differences in the perceived risk of buying online and the effects of receiving a site recommendation', Journal of Business Research, 57 (7), 768-775.

Geeta, D. Vijay (2011), 'Online identity theft – an Indian perspective', Journal of Financial Crime, Vol. 18 No. 3, pp. 235-246.

Gerrard P, Cunningham BJ (2003). The diffusion of internet banking among Singapore consumers. International J. Bank Mark 21(1), 16- 28.

Gerrard, Philip, Cunningham, J., Barton, Devlin, James F. (2006), 'Why consumers are not using internet banking: a qualitative study', Journal of Services Marketing, Vol.20 No.3, pp.160–16.

Giovanis , Apostolos N., Binioris Spyridon and Polychronopoulos, George (2012), 'An extension of TAM model with IDT and security/privacy risk in the adoption of internet banking services in Greece', EuroMed Journal of Business, Vol. 7 No. 1, pp. 24-53.

Hair, J.F., Bush, R.P. & Ortinau, D. J. (2000), Market Research: A practical approach for new Millennium Bostn Irwin/ McGraw Hills.

Hamlet, C. (2000) 'Community banks go online', American Bankers Association. ABA Journal, 92(3).

Ho, Chien-Ta Bruce and Lin, Wen-Chuan (2010), 'Measuring the service quality of internet banking: scale development and validation', European Business Review, Vol. 22 No. 1, pp. 5-24.

Ho, Shu-Hsun and Ko, Ying-Yin (2008), 'Effects of self-service technology on customer value and customer readiness: The case of Internet banking', Internet Research, Vol. 18 No. 4, pp. 427-446. www. mobilereadiness.mastercard.com/the-index.

Hutchinson, Damien and Matthew (2003), 'Security for internet banking: a framework', Logistic information Management, Vol.16, No.1, pp.64-73.

Internet World Stats(2011), Available at http://www.internetworldstats.com/stats3.htm#asia Accessed on 29th September, 2012.

Jagdish Mahapatra (August, 2012), Securing Banking Systems, Business world, available at http://www.businessworld.in/en/storypage/-/bw/securing-banking-systems/509955.0/page/0. Accessed on 3rd September, 2012.

Jaruwachirathanakul, Bussakorn and Fink Dieter (2005), 'Internet banking adoption strategies for a developing country: the case of Thailand', Internet Research, Vol. 15, No. 3, 2005, pp. 295-311.

Joseph, M. and Stone, G. (2003) "An empirical evaluation of US bank Customer Perceptions of the impact of technology on Service delivery in the Banking Sector" International Journal of Retail & Distribution Management, Vol. 31, No. 4, pp. 190-202.

Joseph, M., McClure, C. and Joseph, B. (1999), "Service quality in the banking sector: the impact of technology on service delivery". International Journal of Bank Marketing, Vol.17, No 4, pp 182-191.

Kannabiran, G. & Narayan, P.C.(2005). Deploying internet banking and e-commerce: case study of a private sector bank in India. Information Technology for Development, 11(4), 363-379.

Karjaluoto Heikki, Mattila Minna and Pento Tapio (2002), 'Factor underlying attitude formation towards online banking in Finland', International Journal of Bank Marketing, Vol.20 No. 6, 261-272.

Kesharwani, Ankit and Bisht, Shailendra Singh (2012), 'The impact of trust and perceived risk internet banking adoption in India: An extension of technology acceptance model', International Journal of Bank Marketing, Vol. 30 No. 4, 2012, pp. 303-322.

Krauter, Sonja Grabner and Faullant, Rita (2008), 'Consumer acceptance of internet banking: the influence of internet trust', International Journal of Bank Marketing Vol. 26 No. 7, pp. 483-504.

Laisuzzaman, Ijaj Md., Imran Nahid, Nahid, Abdullah Al, Md. Amin, Ziaul, Md. Abdul Alim (2010), 'The Framework for Implementing ECommerce: The Role of Bank and Telecom in Bangladesh', Journal of Telecommunications, Vo 1 Issue 1, pp. 57-62.

Laukkanen, Sinkkonen, Pekka, Suvi and Laukkanen, Tommi (2008), 'Consumer resistance to internet banking: postponers, opponents and rejectors, The International Journal of Bank Marketing, Vol. 26 No. 6, 2008, pp. 440-455.

Laukkanen, Tommi (2007), 'Internet vs mobile banking: comparing customer value perceptions', Business Process Management Journal, Vol. 13 No. 6, pp. 788-797.

Leblanc, G. (1990), "Customers motivations: use and non-use of automated banking", International Journal of Bank Marketing, Vol. 8, No.4.pp 36-40.

Lewis, B. R. (1991), "Service quality: an international comparison of bank customers' expectations and perceptions", Journal of Marketing Management, Vol. 7, No.1, pp 47-62.

Long, M. and McMellon, C. (2004), "Exploring determinants of retail service quality on the internet". Journal of Service Marketing, Vol. 18, No 1, pp 78-90.

Maditinos, Dimitrios, Dimitrios, Chatzoudes and Lazaros Sarigiannidis (2103), 'An examination of the critical factors affecting consumer acceptance of online banking: A focus on the dimensions of risk', Journal of Systems and Information Technology, Vol. 15 No. 1, pp. 97-116.

Malhotra, Naresh K. (2010), Marketing Research: An Applied Orientation,6th Edition, Prentice Hall Publication.

Malhotra, Pooja and Singh, Balwinder (2007), 'Determinants of Internet banking adoption by banks in India', Internet Research, Vol. 17 No. 3, pp. 323-339

Malhotra, Pooja and Singh, Balwinder (2010), 'An analysis of Internet banking offerings and its determinants in India', Internet Research, Vol. 20 No. 1, pp. 87-106.

Malvika Joshi (2011), Banks' IT spending to surge 50% to Rs 10,000 cr annually, September 8, Available at http://bsl.co.in/india/news/banks-it-spending-to-surge-50-to-rs-10000-cr-annually/448449/, Accessed on 30th September, 2012.

Marshall, J. J. and Heslop, L. A. (1988), "Technology Acceptance in Canadian retail banking: a study of consumer motivations and the use of ATMs", International Journal of Bank Marketing, Vol. 6, No.4.pp 31-41.

Mattila, M., Karjaluoto, H., and Pento, T. (2003). Internet banking adoption among mature customers: early majority or laggards?.Journal of Services Marketing, Vol. 17 No. 5, pp. 514-28.

Mattila, Minna, Karjaluoto, Heikki and Pento, Tapio (2003), 'Internet banking adoption among mature customers: early majority or laggards?' Journal of Services Marketing, Vol. 17 No. 5, pp. 514-528.

Meuter, M. L., Ostrom, A. L., Roundtree, R. I. and Bitner, M. J. (2000), "Self Service Technologies: Understanding Customer Satisfaction with Technology-Based Service Encounter", Journal of Marketing, Vol. 64, July 2000, pp 50-64.

Mols, N. (2000), 'The internet and services marketing: the case of Danish retail banking' Internet research, Electronic networking Application and policy'Vol.10 no1, pp-7-18.

Moscato, Donald R. and Altschuller, Shoshana (2012), 'International Perceptions of Online Banking Security Concerns', Communications of the IIMA,Vol.12 No.3 , pp.51-64.

Mueter, M. L., Ostrom, A. L., Bitner, M. J. and Roundtree, R. I. (2003), "The influence of technology anxiety on consumer use and experience with self-service technologies", Journal of Business Research, Vol 56, No.11, pp 899-906.

Mzoughi, Nabil and Sallem, Wafa M. (2013), 'Predictors of internet banking adoption: Profiling Tunisian postponers, opponents and rejectors', International Journal of Bank Marketing, Vol. 31 No. 5, pp. 388-408.

Narteh, Bedman (2013), ‘Service quality in automated teller machines: an empirical investigation, Managing Service Quality’, Vol. 23 No. 1, 2013, pp. 62-89.

Ndubisi, Nelson Oly and Sinti, Queenie (2006), ‘Consumer attitudes, system’s characteristics and internet banking adoption in Malaysia’, Management Research News, Vol. 29 No. 1/2, 2006, pp. 16-27.

Nitsure, Rupa Rege. "E-banking: Challenges and Opportunities." Economic and Political Weekly (2003): 5377-5381.

Nor, Khalil Md and Mastor, Nor Hamimah (2010), ‘Malay, Chinese, and internet Banking’, Chinese Management Studies, Vol. 4 No. 2, pp. 141-153.

Nunnally, J. (1978) Psychometric theory, New York, McGraw-Hill.

Patsiotis, Athanasios G., Hughes, Tim and Webber, Don J., (2012), ‘Adopters and non-adopters of internet banking: a segmentation study’, International Journal of Bank Marketing, Vol. 30 No. 1, pp. 20-42.

Pikkarainen, T., Pikkarainen, K., Karjaluoto, H., &Pahnila, S. (2004). Consumer acceptance of online banking: An extension of the technology acceptance model. Internet Research, 14 (3), 224-235.

Polasik, Michal and Wisniewski, Tomasz Piotr (2009), ‘Empirical analysis of internet banking adoption in Poland’, International Journal of Bank Marketing, Vol. 27 No. 1, 2009, pp. 32-52.

Polatoglu VN, Ekin S (2001). An empirical investigation of the Turkish consumers' acceptance of internet banking services. International J. Bank Mark. 19(4): 156-165.

Polatoglu,Vichuda Nui and Ekin, Serap (2001), ‘An empirical investigation of the Turkish consumers' acceptance of Internet banking services’, International Journal of Bank Marketing, Vol.19 No.4, pp.156-165.

Poon, Wai-Ching (2008), 'Users' adoption of e-banking services: the Malaysian perspective' Journal of Business & Industrial Marketing, Vol.23 No.1, pp.59–69.

PWC (2012), Carving a new path through innovation, CII Banking Tech Summit report. Available at https://www.pwc.com/in/en/assets/pdfs/consulting/financial-services/Carving_a_New_Path_Through_Innovation_June_28_2012.pdf , Accessed on 9th September, 2012.

Rajneesh De and Padmanabhan, Chitra, (2002), "Internet Opens New Vistas for Indian Banking", Express Computer, 16th September, available at http://www.expresscomputeronline.com/20021202/banks1.shtml. Accessed on 9th September, 2012.

RBI (2012), Report on Trend and Progress of banking in India.

RBI's Report of Internet banking (2001) available at http://rbidocs.rbi.org.in/rdocs/notification/PDFs/21569.pdf

Reserve Bank of India (2001), Report on Internet Banking, Available http://rbidocs.rbi.org.in/rdocs/PublicationReport/Pdfs/21595.pdf Accessed on September 5, 2012.

Rod Michel, Ashill, Nicholas J., Shao, Jinyi and Carruthers, Janet (2009), 'An examination of the relationship between service quality dimensions, overall internet banking service quality and customer satisfaction: A New Zealand study, Marketing Intelligence & Planning, Vol. 27 No. 1, pp. 103-126.

Rugimbana, R. and Iversen, P. (1994), "Perceived attributes of ATMs and their marketing implications", International Journal of Bank Marketing, Vol. 12 No. 2, pp. 30-5.

SafeenaRahmath, AbdullahHema Date (2010) Customer Perspectives on E-business Value: Case Study on Internet Banking, Journal of Internet Banking and Commerce, Vol.15, No.1, e-journal, available at http://www.arraydev.com/commerce/jibc/2010-04/Rahmath%20Safeena.pdf Accessed on10th September,2012.

Salhieh, Loay, Abu-Doleh, Jamal and Hijazi, Nada (2011), 'The assessment of e-banking readiness in Jordan', International Journal of Islamic and Middle Eastern Finance and Management, Vol. 4 No. 4, pp. 325-342 .

Sarel, D., & Marmorstein, H. (2003a). Marketing online banking services: The voice of the customer. Journal of Financial Services Marketing, 8 (2), 106–118.

Sathye, Milind (1999), 'Adoption of Internet banking by Australian consumers: an empirical investigation', International Journal of Bank Marketing, Vol.17, No.7, pp.324-334.

Sayar, Ceren, Wolf Simon (2007), 'Internet banking market performance: Turkey versus the UK', International Journal of Bank Marketing, Vol. 25 No. 3, pp. 122-141.

Shih, Ya-Yueh and Fang, Kwoting (2004), 'The use of a decomposed theory of planned behavior to study Internet banking in Taiwan', Internet Research, Vol. 14 No.3, pp. 213–223.

Singh Tejinderpal, Kaur Manpreet (2012), Internet Banking: Content Analysis Of Selected Indian Public And Private Sector Banks' Online Portals, vol. 17, No. 1, pp. 1-7.

Singhal, D., & Padhmanabban, V. (2008). A study of customer perception toward internet banking: Identifying major contributing factors. The Journal of

Nepalese Business Studies, 5(1), 101-111. [Online] Available: http://www.nepjol.info/index.php/JNBS/article/view/2088 Accessed on September 5, 2012.

Srivastava, Rajesh Kumar (2007), Customer's perception on usage of internet banking, Innovative Marketing, Volume 3, Issue 4, 2007,67-73.

Subsorn P. and Limwiriyakul S. (2012), A Comparative Analysis of Internet Banking Security in Thailand: A Customer Perspective, Procedia Engineering 32, 260-272.

Surulivel, S. T., and B. Charumathi. "Impact of Information Technology (IT) Investments on the Cost Efficiency of Indian Banking Sector-A Stochastic Frontier Approach (SFA)." International Journal of Engineering and Technology (2013).

Thakur, Rakhi and Srivastava, Mala (2013), 'Customer usage intention of mobile commerce in India: an empirical study', Journal of Indian Business Research Vol. 5 No. 1, pp. 52-72.

Tommi, Laukkanen and Vesa, Kiviniemi (2010), 'The role of information in mobile banking resistance', International Journal of Bank Marketing, Vol. 28 No. 5, pp. 372-388.

Wan Wendy W.N., Luk Chung-Leung and Chow Cheris W.C.(2005), 'Customers' adoption of banking channels in Hong Kong', International Journal of Bank Marketing, Vol. 23 No. 3, pp. 255-272.

Wang, Yi-Shun, Wang, Yu-Min, Lin, Hsin-Hui and Tang, Tzung-I (2003), 'Determinants of user acceptance of Internet banking: an empirical study', International Journal of Service Management, Vol. 14 No. 5, pp. 501-519.

Wessels Lisa and Drennan Judy (2010), 'An investigation of consumer acceptance of M-banking', International Journal of Bank Marketing, Vol. 28 No. 7, pp. 547-568.

Yang, Z. and Jun, M. (2002), "Consumer perception of e-service quality: from internet purchase and non Purchase Perspectives", Journal of Business Strategies, Vol.19 No1, pp 19-41.

Yap, Kenneth B., Wong David H., Loh, Claire and Bak, Randall (2010), Offline and online banking-where to draw the line when building trust in e-banking? International Journal of Bank Marketing, Vol. 28 No. 1, pp. 27-46.

Yousafzai, Shumaila and Soriano, MirellaYani-de (2012), 'Understanding customer specific factors underpinning internet banking adoption', International Journal of Bank Marketing, Vol. 30 No. 1, pp. 60-81.

Zeithaml, V.A. and Gilly, M.C. (1987), "Characteristics affecting the acceptance of retailing technologies: a comparison of elderly and non-elderly consumers", Journal of Retail Banking, Vol. 63 No.1, pp. 49-68.

Zhao, Anita Lifen and Lewis, Nicole Koenig,(2010), 'Adoption of internet banking services in China: is it all about trust?', International Journal of Bank Marketing, Vol. 28 No. 1, pp. 7-26.

Zhou, Tao (2011), 'An empirical examination of initial trust in mobile banking, Internet Research', Vol. 21 No. 5, pp. 527-540.

Zhu,Yu-Qian and Chen, Houn-Gee (2012), 'Service fairness and customer satisfaction in internet banking: Exploring the mediating effects of trust and customer value', Internet Research, Vol. 22 No. 4, pp. 482-498.

Internet Resources

www.alexa.com

www.charts.medianama.com/india-mobile-banking-transactions

www.hdfcbank.com

www.icicibank.com

www.Internetworldstats.com

www.mckinsey.com

www.mobilereadiness.mastercard.com/the-index.

www.msn.encarta.com

www.netbanking.hdfcbank.com/netbanking

www.netpnb.com

www.onlinesbi.com

www.pnbindia.in

www.rbi.org.in

www.sbi.co.in

Annexure-I
Check List
Pre-Login and Post Login Feature of Online Banking Portals

Sr. No.	Pre-Login Features	Public Sector Banks		Private Sector Banks	
		SBI	PNB	ICICI	HDFC
xi.	Direct access from bank's main home page				
xii.	OTP requirement, if logging from different computer or browser				
xiii.	Availability of Virtual Keyboard				
xiv.	Availability of Scrambled Keyboard				
xv.	Availability of Scrambled Keyboard with 'Shuffle' option				
xvi.	Availability of Hovering Keyboard				
xvii.	Multi-Factor Authentication (MFA)				
xviii.	Alert of leftover attempts in case of wrong passwords				
xix.	Security Alerts/ Warning message at login page				
xx.	SSL certificate (encryption) SSLBit				
	Post Login Features				
i.	Expiry of User ID, if not used				
ii.	Expiry of Login Password				
iii.	Expiry of Transaction Password				
iv.	Last Login date and Time				
v.	Mandatory 'Profile Password' to add new payee				
vi.	OTP to add payee				
vii.	Mandatory 'URN' at the time of Online payments				
viii.	Assigning Maximum fund transfer limit to an account				
ix.	Debit Card Grid Authentication to add payee				
x.	Mobile alert				
xi.	Reset Transaction Password online				
xii.	Idle Time log out				
xiii.	'Backspace'' Fresh' ' Forward' Logout				

Annexure -II

Survey on

'**Security and Privacy Issues in E- Banking: An Empirical Study of Customers' Perception'**

Section-I(Demographic Profile)

Tick (√) in the appropriate Box

Name of your Primary Bank (Only one Please)	State Bank of India State Bank of Patiala Punjab National Bank HDFC Bank Ltd. ICICI Bank Ltd. Axis Bank Ltd. Any Other (Specify).....	□ □ □ □ □ □
Educational Qualification	Undergraduate Graduate Postgraduate Doctorate Others (specify)……..	□ □ □ □
Age	_____Years	
Gender	Male Female	□ □

Family Income (Rs/ Month).	Less than 40000 40000-60000 60000-80000 80000- 100000 More than 100000	□ □ □ □ □
Occupation	Professional Businessperson Service House Wife Others (specify)……	□ □ □ □ □
Mobile Phone	Classic Phone Smart Phone	□ □
Internet Connection at Home	Yes No	□ □

Section-II (ATM)

1	Which of the following new technology based banking channels are you aware? (*you may tick more than one option*)	1. ATM 2. Internet Banking 3. Phone Banking 4. Mobile Banking	□ □ □ □
2	Do you use ATM?	1. Yes 2. No	□ □
If 'YES', Please answers the following questions with respect to ATM of your Primary Bank, otherwise go to **Question Number 8**			
3	Since how long are you using ATM?	1. Less than 1 year 2. 1 - 2year 3. 2-4 years 4. 4-6 years 5. More than 6years	□ □ □ □ □
4	How often do you use ATM?	1. More than once in a week 2. Once in a week 3. Once in Fortnight 4. Once in a month 5. Once in a quarter	□ □ □ □ □
5	Following statements measure your level of concern for 'security and privacy' with respect to use of ATM in general. Please rate each statement ranging from **'Strongly Agree'** to **'Strongly Disagree'**		

	Statement	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
5.1	My ATM password may be stolen	5	4	3	2	1
5.2	My ATM card may be cloned (duplicated)	5	4	3	2	1
5.3	My ATM may dispense less amount of currency than requested by me	5	4	3	2	1
5.4	Someone may withdraw cash from my ATM without using my card	5	4	3	2	1
5.5	Someone can transfer cash from my ATM without using my card	5	4	3	2	1
5.6	There may be deduction in my balance without any transaction	5	4	3	2	1
5.7	My card information may be shared by the bank with Third party	5	4	3	2	1
5.8	Others may see my password while entering it	5	4	3	2	1
5.9	I will not get my card back if stuck in ATM	5	4	3	2	1
6	Please rate the following statement on the basis of your perception regarding security and privacy level of **your bank's ATMs**					
	Statement	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
6.1	It is safe to withdraw the cash from my banks' ATMs	5	4	3	2	1
6.2	My PIN can't be hacked while using my banks' ATMs	5	4	3	2	1
6.3	It is not possible for others to see my password while entering	5	4	3	2	1
6.4	My ATM card can't be cloned (Duplicated)	5	4	3	2	1
6.5	My Bank guides me about security tips from time to time	5	4	3	2	1
6.6	There is limit of maximum number of incorrect password submissions	5	4	3	2	1
6.7	Contact information is easily available to block my ATM card	5	4	3	2	1
6.8	Door of the ATM Cabin has secure access	5	4	3	2	1
6.9	There is adequate privacy while using ATM	5	4	3	2	1
6.10	Only one person is allowed to enter ATM Cabin for transaction.	5	4	3	2	1
7	Please rate you overall satisfaction about the ATM services of your Bank	1. Highly Satisfied 2. Satisfied 3. Neutral 4. Dissatisfied 5. HighlyDissatisfied				□ □ □ □ □
8	Please tick the reason(s) for not using ATM? **(This question is for Non-ATM users)**	1. Don't not know how to use 2. It is not a secured channel 3. Not clear about the benefits of using ATMs 4. There is lack of privacy while using ATM 5. Any other reason (Specify) ----------				□ □ □ □
Section-III(Internet Banking)						
9	Do you use Internet Banking?	1. Yes 2. No				□ □

If 'YES' Please answers the following questions with respect to Internet banking of you Primary Bank, otherwise go to **Question Number 18**			
10	How often do you use internet banking?	1. More than once in a week 2. Once in a week 3. Once in a Fortnight 4. Once in a month 5. Once in a quarter	□ □ □ □ □
11	For what purpose do you internet banking? (You may tick more than one option)	1. Checking of Balance 2. Checking of Mini Statement 3. Transfer of Funds 4. Payment of Bills 5. Online shopping 6. Any Other (Please Specify) ----------	□ □ □ □ □
12	In your opinion, please rate the strength of your internet banking password?	1. Very Strong 2. Strong 3. Neither strong nor weak 4. Weak 5. Very weak	□ □ □ □ □
13	Which of the security feature(s) of internet banking are you aware of ?	1. One time password (OTP) 2. Profile password 3. Virtual key board 4. Hyper Text Transfer Protocol secured (https)	□ □ □ □
14	Are you aware of virtual Keyboard?	1. Yes 2. No	□ □
	If' 'Yes' Please answer		
	How many times do you use virtual key board to enter Login ID and password?	1. Never 2. Sometimes 3. Frequently 4. Always	□ □ □ □
	Did your bank ever approach you to explain the significance of Virtual Key board	1. Yes 2. No	□ □
	Which of the following types of Virtual key board are you aware (tick)	1. **Scrambled Keyboard** 2. **Hovering Keyboard**	□ □

15 Following statements measure your level of concern for security and privacy with respect to use of **Internet Banking**. Please rate each statement ranging from 'Strongly Agree' to 'Strongly Disagree'

	Statement	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
15.1	My internet banking password may be stolen	5	4	3	2	1
15.2	Funds may be fraudulently transferred from my account to other's account	5	4	3	2	1
15.3	I may provide internet banking password at fake websites by mistake	5	4	3	2	1
15.4	One can monitor my financial transaction history	5	4	3	2	1
15.5	Bank will not refund my money back if there is online fraud	5	4	3	2	1
15.6	My account related may be shared by the bank with third party	5	4	3	2	1
15.7	My online behaviour may be shared with third party	5	4	3	2	1

15.8	Internet banking is vulnerable to fraud	5	4	3	2	1

16	Please rate the following statement on the basis of your perception regarding security and privacy level of **your internet banking.**					
	Statement	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
16.1	It is safe to use internet banking of my bank	5	4	3	2	1
16.2	The site has virtual keyboard to enter Password and User ID	5	4	3	2	1
16.3	The site provides security guidelines on home page	5	4	3	2	1
16.4	OTP(One Time Password) is required, if logging from different browsers/computers	5	4	3	2	1
16.5	OTP is required while making Third Party payments	5	4	3	2	1
16.6	OTP is always required while adding beneficiary	5	4	3	2	1
16.7	Pressing back space results in immediately logout from session	5	4	3	2	1
16.8	Idle time log out from session exists at my Bank's site	5	4	3	2	1
16.9	There is maximum number of incorrect password submissions	5	4	3	2	1
16.10	Bank provide me the facility of choosing strong password for internet banking	5	4	3	2	1
16.11	Bank remind me to change password from time to time	5	4	3	2	1

17	Please rate you overall satisfaction about the Internet banking services of your principle bank	1. Highly Satisfied 2. Satisfied 3. Neutral 4. Dissatisfied 5. Highly Dissatisfied	□ □ □ □ □
18	Please tick the reason(s) for not using Internet Banking? **(This question is for Non-internet Banking users)**	1. Don't not know how to use 2. It is not a secured channel 3. There is lack of privacy while using internet banking 4. Any other reason (Specify) _____	□ □ □
	Section- IV (Mobile Banking)		
19	Do you use Mobile Banking?	Yes No	□ □
If Answer is 'YES' Please answers the following questions otherwise go to **Question Number 26**			
20	How do you use Mobile Banking?	1. Through Browser 2. Through Mobile Banking Application 3. Through SMS	□ □ □
21	How often do you use Mobile banking?	1. More than once in a week 2. Once in a week 3. Once in a Fortnight 4. Once in a month 5. Once in a quarter	□ □ □ □ □
22	For what purpose do you use Mobile banking?	1. Checking of Balances 2. Checking of Mini Statement 3. Transfer of Funds 4. Payment of Bills 5. Online Shopping 6. Any Other (Please Specify) _____	□ □ □ □ □

23	The following statements measure your level of concern for security and privacy with respect to use of Mobile Banking. Please rate each statement ranging from **'Strongly Agree'** to **'Strongly Disagree'**					
	Statement	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
23.1	My mobile banking password may be stolen	5	4	3	2	1
23.2	Funds may be fraudulently transferred by using mobile banking	5	4	3	2	1
23.3	I may provide mobile banking password at fake websites by mistake	5	4	3	2	1
23.4	Mobile service providers may monitor my financial transaction.	5	4	3	2	1
23.5	It is very easy for others to 'Add payee' form my mobile banking account	5	4	3	2	1
23.6	Bank will not refund my money back if there is online fraud	5	4	3	2	1
23.7	My personal information may be shared by the bank with third party	5	4	3	2	1
23.8	Mobile banking is vulnerable to fraud	5	4	3	2	1
23.9	If my phone is stolen, someone else can use my mobile banking	5	4	3	2	1
23.10	My confidential mobile banking information may be accessed by others through blue tooth	5	4	3	2	1
24	Please rate the following statements ranging from 'strongly agree' to 'strongly disagree' on the basis of your perception **about security and privacy level of your primary Banks's mobile banking**					
	Statement	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
24.1	It is safe to use mobile banking of my Bank	5	4	3	2	1
24.2	Security guidelines are displayed before using Mobile banking	5	4	3	2	1
24.3	There is maximum number of incorrect password submissions	5	4	3	2	1
24.4	My Bank provide me the facility of choosing strong password	5	4	3	2	1
24.5	OTP (One Time Password) is always required while making Third Party payments	5	4	3	2	1
24.6	OTP is always required while adding payee account on my site	5	4	3	2	1
24.7	Pressing back space results in immediately logout from session	5	4	3	2	1
24.8	Idle time log out from session exists at my Bank's site	5	4	3	2	1
24.9	My bank does not share my personal information with other sites	5	4	3	2	1
24.10	My mobile banking site protects information about my onsite behaviour	5	4	3	2	1
25	Please rate you overall satisfaction about the Mobilebanking of your Bank	1. Highly Satisfied 2. Satisfied 3. Neutral 4. Dissatisfied 5. Highly Dissatisfied				□ □ □ □ □
26	Please tick the reason(s) for not **using**Mobile Banking? **(This question is for Non-Mobile Banking users)**	1. Don't not know how to use 2. It is not a secured channel 3. There is lack of privacy while using Mobile banking 4. Any other reason (Specify)				□ □ □

		_____	
Section-V (Credit Cards)			
27	Do you use Credit card ?	1. Yes 2. No	□ □
	If 'YES' , Please answers the following questions otherwise go to **Question Number 32**		
28	Where do you use credit card (at)?	1. Physical Shops 2. Online 3. Both	□ □ □
29	Following statements measure your level of concern for security and privacy with respect to use of Credit Cards.		

	Statement	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
29.1	My credit card information may be stolen	5	4	3	2	1
29.2	My credit card may be used by others without having my card	5	4	3	2	1
29.3	I may provide credit card information on fake websites	5	4	3	2	1
29.4	CVV(password) of my card may be stolen	5	4	3	2	1
29.5	My card usage information may be shared by bank with others	5	4	3	2	1
30	Please rate the following statements ranging from 'Strongly agree' to 'Strongly disagree' on the basis of your perception about security and privacy level **of your credit card**					

	Statement	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
30.1	It is safe to use credit card of my bank	5	4	3	2	1
30.2	Security guideline are always there to use a card	5	4	3	2	1
30.3	Online usage of card is secure	5	4	3	2	1
30.4	I always get mobile message for my credit card transaction	5	4	3	2	1
30.5	CVV of my card can't be hacked	5	4	3	2	1
30.6	My credit card bill always shows the correct amount spent by me	5	4	3	2	1
30.7	My credit card information is safe	5	4	3	2	1
30.8	My bank does not share my card usage information with others	5	4	3	2	1

31	Please rate you overall satisfaction about the credit card service of your Bank	1. Highly Satisfied 2. Satisfied 3. Neutral 4. Dissatisfied 5. Highly Dissatisfied	□ □ □ □ □
32	Please tick the reason(s) for not using Credit card **(This question is for Non-Credit card users)**	1. Don't not know how to use 2. It is not a secured channel for payment 3. There is lack of privacy while using it 4. Any other reason (Specify) _____	□ □ □ □

33	Please give suggestion(s) to make e-banking more secure.	