Indian Management Studies Journal 18 (2014) 125-141

Indian
Management
Studies Journal

Is Internet Banking in India Safe?
(A Comparative Study of Public, Private and Foreign Sector Banks)

Dhiraj Sharma* and Tejinder Pal Singh Brar**

* *School of Management Studies, Punjabi University, Patiala*

** *Department of Computer Applications, Chandigarh University, Punjab*

Abstract

The usage of internet banking has grown tremendously over the past several years and will continue to grow as the banks continue to allow customers to perform variety of transactions through their web portals. On the other hand, internet banking has its own issues like security, privacy, confidentiality and integrity. There are also a number of cyber crimes and attacks like phishing, smishing, pharming, spyware, malware etc. that attempt to steal customer information. The bank customers do not have any option of making a choice of a bank depending on the strength of internet banking security features. This paper studies and examines the internet banking security features provided by the selected public, private and foreign sector banks in India.

Key Words

Internet Banking, Security, Phishing, Smishing, IDS, Encryption, Pharming

INTRODUCTION

In India too, internet banking has grown and flourished over the years. It is a highly profitable channel for financial institutions. Success of a financial institution depends on a number of factors like business strategy, service delivery, business model, teamwork and so on. But technology plays an important role in the success of any financial organization. Through internet banking a bank can deliver innovative products and services to its customers. Multichannel strategies can help banks to lower their costs and increase business process and innovation (Rossignoli and Zardini, 2013). Increasing competition has become a challenge for banks but the technology holds the key to success of banks (Kaur, 2012). With any type of technology, security always remains an issue and banks now face major threat due to the security issues. Security is a threat that creates a situation, with the potential to cause economic hardship to data or network resources in the form of destruction, disclosures, and modification of data, denial of service, and fraud (Kalakota and Whinston, 1997).

Recently, there has been a considerable rise in the security issues which significantly affect the bank customers and their confidence in the financial institution along with bank reputation and trustworthiness. Sathye (1999) found that 73% customers avoided the adoption of online banking because they are concerned about safety and security of transactions over the internet. On the similar lines, Al-Somali et al. (2008) concludes that security and reliability of transactions over the internet are important factors that customer considers before adopting online banking. Customers avoid online banking as they perceive it as being easily vulnerable to fraud. Financial institutions always have been based on trust and protecting the private information of a customer is vital for the banks (Jayaraman and Ernest, 2012). Banks offering online services should have effective and reliable methods to authenticate customers. These methods are required to reduce fraud, protect customer information and identity theft. The future challenges for the adoption of online banking are security, privacy, bank reputation and regulations (Aladwani, 2001). There are a number of factors which affect the customer's perception about security in online banking. These include phishing / smishing attacks, the increased usage of pharming, malware, spyware and widespread data security breaches. A report published by the world's largest technology research firm Gartner (2005), indicates that millions of consumers unintentionally fall for phishing attacks estimated 57 million adults in US have received e-mail attacks in 2004 from phishers/hackers/cyber thieves who try to steal customer account information such as credit card information, home addresses and telephone numbers. On the same lines, in a study published by RSA (2005), two separate surveys have shown the concerns of customers over online security and identity protection. The first study found that trends such as data breaches, phishing and pharming have affected customer's behavior and perception towards online banking. According to another study, nearly one-fifth of customers surveyed refused to utilize their financial institution's internet products. Over fifty per cent consumers considered the user ID and password not enough to protect their online information. A survey conducted by Watchfire Corporation (2005), focused on the relationship between customer trust and usage in online banking. The study found that customers having a high level of trust in their financial institutions are more likely to use online banking services and likely to remain loyal with their bank. However, customers who trusted their bank would take their business to another bank if their existing bank had even one security violation. This indicates that any privacy or data security violation can have severe economic impacts on a financial institution.

The security (rather lack of it) is a main barrier to e-commerce expansion and it is the most feared problem on the internet and customers take a very high risk by dealing electronically (Mukti, 2000). On the other hand, Grethen (2001) found that communication across an open and insecure channel is not the best option for bank-client relations as trust may be lost. After analyzing different research studies, Fitzergerald (2004) argued that lack of awareness of internet banking and the security concerns are the major non-adoption factors for internet banking. Liao and Cheung (2003) concludes that willingness to use internet banking depends upon the number of factors such as accuracy, security, network speed, user-friendliness, user-involvement, and convenience. There are a number of researches and studies [(Usman and Shah, 2013), (Kesharwani and Radhakrishna, 2013), (Malhotra and Singh,2009),(Symantec Corporation, 2005), (Bauer et al., 2005), (White and Nteli, 2004)] that have focused on internet banking security. Financial organizations such as banks face greater risk of unauthorized access to their computer or network. However, the online banking system users face the security risks with unauthorized access into their banking accounts. Therefore, it is extremely important to build in non-reputability i.e. identity of both the sender and the receiver can be attested by a trusted third party who holds the identity certificates. The Reserve Bank of India (RBI) in 2011 has set up a working group on "information security, online banking, technology risk management and cyber frauds" to examine different aspects of online banking. The Group has focused on these major areas (i) IT governance (ii) information security (iii) legal issues (iv) cyber frauds. RBI is implementing the recommendations of the group in a phased manner.

OBJECTIVES AND RESEARCH METHODOLOGY OF THE STUDY

The objective of this paper is to explore the security potential of Indian banks' web portals through which they offer internet banking services. A bank's website is an interactive media through which it communicates and transacts with its customers. The information displayed on web page can be used to evaluate the internet banking security features and their strength. Therefore, the existing customer base can use this information to identify security strengths and weaknesses. On the other hand, the potential online banking customers can be provided with security information and an idea of internet banking security prior to the selection of a bank.

The present paper, using a qualitative approach, investigates the security features that are available on Indian bank's web portals. To accomplish this objective, 12 Indian commercial banks - four each from Public, Private and Foreign sector banks has been selected randomly. All of these selected banks have their banking websites and provides internet banking services. The data has been collected from primary as well as secondary sources. For collection of primary data, the branches of selected banks have been visited and data has been collected from IT managers, system analysts and IT help desk. Secondary data has been collected through the web portals of selected banks. The comparative analysis is compiled into two major classes - (1) the availability of E-banking security features of the selected Indian banks (2) the difference and variations in the security features of selected banks. All the data pertaining to the websites was collected and analyzed during the period between January to April 2014. The list of Indian banks under study is displayed in Table 1 and the Categories of Security Features are listed in Table 2.

Table 1
List of Selected Indian Commercial Banks

Sr. No.	Group-I Public Sector Banks	Group-II Private Sector Banks	Group-III Foreign Sector Banks
1.	State Bank of India (SBI)	Housing Development Finance Corporation (HDFC) Bank	Hongkong & Shanghai Banking Corporation (HSBC)
2.	Bank Of Baroda (BOB)	Industrial Credit and Investment Corporation of India (ICICI) Bank	Citibank India
3.	Punjab National Bank (PNB)	Indusind Bank Limited	Standard Chartered Bank (SCB)
4.	United Commercial Bank (UCO)	Kotak Mahindra Bank	American Express Bank (AEB)

Table 2
Categories of Security Features

Category	Security Features
1	General information on online security and privacy
2	Information technology (IT) assistance and support
3	Software and system requirements
4	Bank site authentication technology
5	User site authentication technology
6	Internet banking application security features

The details of each of these categories, as displayed in Table 2, are explained below :

Category 1 : General Online Security and Privacy Information

- This category investigates the current privacy and confidentiality policy which the banks provide to the internet banking customers. The policy must comply with privacy laws provided by RBI (2011) in order to ensure the integrity of the online banking customer's confidential information.
- It also examines current guarantee policy where the banks are obliged to cover any losses in case unauthorized transactions.
- This category inspects the internet security information which is provided by the banks to their customers such as security threats, guidelines and tips.
- This category attempts to identify whether the banks supply information on their security systems such as firewalls and intrusion detection systems etc.

Category 2 : IT Assistance and Customer Care Support

This category consists of availability of customer care or helpdesk services provided by banks. In order to identify information related to customer care or helpdesk support, banks' websites need to be checked. The banks should provide a number of different modes of communication with the online banking customers.

Category 3 : Software and System Requirements

This category is comprised of three parts :

- Security software/tool available to the online banking customers
- Compatibility with the number of popular internet browsers
- Online banking user device and browser setting requirement

Category 4 : Bank Site Authentication Technology

This involves an identification of the bank authentication technology which is currently implemented by bank to cover types of digital certificate technology, SSL encryption and certificate authority.

Category 5 : User Site Authentication Technology

This category is concerned with identifying authentication technologies that are provided by banks to internet banking customers. It consists of the following :

- Logon requirements
- Logon failure limits
- Logon user input type
- Password restrictions
- Transaction verification

Category 6 : Internet Banking Application Security Features

This category shows the following security features of the banks' internet banking applications :

- Logging information- includes last login information such as the date and time.
- Default daily transfer amount- finds out a default daily transfer amount limit.
- Automatic timeout- identifies a default automatic timeout setting limit.

RESULTS AND ANALYSIS

Table 3 reveals the major web security features offered by banks under study. Following is the brief discussion of various security category features of different bank groups under study.

Category 1 : General Online Security and Privacy Information

All of the selected banks have found to be fully complying with the RBI's present Privacy Laws. All the banks have been certain constraints of liability for any claim/ loss/damage on the use of the internet banking services. Most of them take responsibility only in the following situations :

- Erroneous/Unauthorized debiting of account
- ECS direct debits/other debits to accounts
- Violation of the code by bank's agent
- Compensation for loss of instrument in transit
- Foreign exchange services
- Reversal of erroneous/unauthorized/fraudulent or other transactions
- Cheque/Instruments lost in transit/in clearing process or at paying bank's branch
- Payment of interest for delay in issue of duplicate draft
- Delay in crediting failed ATM transactions
- Force Majeure (chance occurrence or unavoidable accident)

Table 3

Internet Banking Security Strength of Selected Indian Commercial Banks

Security Feature Categories	Group-I				Group-II				Group-III			
	Public Sector Banks				Private Sector Banks				Foreign Banks			
	SBI	BOB	PNB	UCO	HDFC	ICICI	INDUSIND	KOTAK	HSBC	CITIBANK	SCB	AEB
1. General Online Security and Privacy Information												
Bank Complying with RBI Privacy Laws	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES
Compensation Policy	C	C	C	C	C	C	C	C	C	C	C	C
General Security Guideline	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES
Security Information for Threats	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES
Keylogger	NI	NI	NI	NI	NI	NI	NI	NI	NI	NI	NI	NI
Bank Security Mechanism (Firewall)	YES	NI	YES	NI	YES	YES	YES	YES	YES	NI	YES	NI
IDS	YES	NI	YES	NI	YES	YES	NI	NI	NI	NI	NI	NI
2. IT Assistance and Customer Care Support												
24/7 Customer Contact Centre (by Phone)	YES	YES	YES	NI	YES	YES	YES	YES	L	YES	YES	YES
Secured Email	NI	NI	YES	YES	NI	YES	NI	NI	NI	NI	YES	NI
FAQ / Online Support Form	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES
3. Software and System Requirements												
3.1 Security Software / Tool Available												
Anti-virus / Anti-Spyware	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA

Contd.

Contd. Table 3

3.2 Compatability with Internet Browsers												
IE	YES	YES	NI	YES	YES	YES	YES	YES	YES	NI	YES	YES
Chrome	YES	NI	NI	NI	YES	YES	YES	YES	NI	NI	YES	NI
Mozilla	YES	NI	NI	NI	NI	NI	NI	NI	NI	NI	NI	NI
Firefox	NI	NI	NI	NI	YES	NI	NI	YES	NI	NI	YES	NI
Netscape	NI	NI	NI	NI	NI	YES	NI	NI	YES	NI	NI	YES
3.3 Internet Banking User Device System and Browser Setting Requirement												
Operating System	YES	YES	YES	NI	YES	YES	YES	NI	YES	YES	YES	NI
Type of Browser Setting (e.g. java, cookie)	YES	YES	NI	NI	NI	YES	NI	NI	YES	NI	NI	YES
Screen Resolution	YES	YES	NI	YES	YES	NI	NI	YES	YES	NI	NI	NI
4. Bank Site Authentication Technology												
SSL Encryption	256 bit	128 bit	128 bit	128 bit	128 bit	128 bit	128 bit	128 bit	128 bit	128 bit	256 bit	YES
CA	VS	VS	VS	NI	VS	Entrust	VS	Entrust	NI	VS	NI	NI
5. User Site Authentication Technology												
5.1 Logon Requirments												
Customer ID	USER	YES	YES	YES	YES	YES	NI	YES	YES	YES	YES	YES
Password	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES
Two Factor Authentication	YES	NI	YES	NI	NI	YES	NI	NI	YES	YES	NI	YES
5.2 Logon Failure Limits												
Maximum Limits	YES	NI	YES	YES	YES	YES	YES	YES	YES	NI	YES	YES

Contd. Table 3

5.3 Logon User Input Type												
Keyboard	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES
On screen/Virtual Keypad	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES
5.3 Password Restriction	YES	YES	YES	NI	YES	YES	NI	NI	YES	NI	YES	NI
5.4 Transaction Verification	YES	NI	NI	NI	YES	YES	NI	NI	NI	YES	NI	NI
6. Internet Banking Application Security Features												
Logging Information	YES	NI	YES	YES	YES	YES	NI	NI	NI	YES	YES	YES
Default Daily Transfer Limit	YES	YES	YES	YES	YES	YES	NI	NI	YES	NI	NI	YES
Automatic Timeout	YES	NI	YES	NI	YES	YES	YES	YES	YES	YES	YES	YES

C = Conditional, NI = No Information, NA = Not available, VS = Veri Sign authentication, L = Limited

[i] Phishing is the act of attempting to acquire sensitive information such as credit card details, username and password.

[ii] Smishing is a type of phishing technique in which phishing is done through SMS (Short Message Service). It is a form of criminal activity which uses social engineering techniques.

[iii] Pharming is a cyber attack which redirects a website's traffic to another fake website.

[iv] Malware (short for malicious software), is a software used to interrupt computer operation, collect sensitive information or gain access to private computer systems.

[v] Spyware is a software that aids in gathering information about a person or organization without their knowledge

[vi] It is the process of recording or logging the keys that struck on a customer keyboard, where the customer is unaware that their actions are being monitored.

[vii] It is a system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both.

[viii] IDS (Intrusion Detection systems) is a software application or device that monitors network or system activities for malicious activities or policy violations and produces reports to a management station.

If it is proven that the fraud/omission/ negligence or wilful act has been caused by the bank or bank employee, then liability is limited to the amount of the relevant transaction/ amount of the direct loss or actual damage (whichever is less). Otherwise, the bank will not assume any responsibility and the loss will be borne by the customers.

Majority of the banks are providing useful general internet security information on their websites along with security information for various types of threats like phishing/spyware/hacking/online frauds/pharming/smishing. We found that no bank under study is providing the information on Keyloggers . Information on security mechanism like firewall has not given by four banks (BOB, UCO, AEB and CITIBANK) whereas IDS was found to be available with only four banks (SBI, PNB, HDFC and ICICI). No information about IDS is being provided by the remaining six banks. The provision of security mechanism information can increase internet banking security awareness and confidentiality assurance to internet banking users.

Under Category 1 concerning general information on online security and privacy, out of Group-I (Public Sector Banks) SBI and PNB top the group by providing maximum general information on security and privacy issues like compliance with RBI guidelines, general security guidelines, information about various threats, bank security mechanism and IDS. However, BOB and UCO banks lag behind as they are providing minimum general information on security and privacy. From Group-II banks (Private Banks), ICICI Bank and HDFC Bank top the group by providing maximum general information on security and privacy. IndusInd and Kotak Mahindra banks lag behind as they provide lesser general information on security and privacy. From Group-III banks (Foreign Banks), HSBC and Standard Chartered Bank top the category by providing maximum general information on security and privacy features while Citibank and American Express Bank lags behind as they provide lesser general information on security and privacy.

Category 2 : IT Assistance and Customer Care Support

The majority of banks are providing 24X7 telephone support while this information is not provided by three banks (UCO, AEB and HSBC). On the other hand, majority of the banks provide several types of IT assistance and support such as demo, FAQ, and online support through their online banking websites.

Under Category 2, out of Group-I (Public Sector Banks) PNB tops the group by providing maximum services like 24 × 7 telephonic support, secured mail and FAQ/online support. While SBI, BOB and UCO banks lag behind as they provide less information, IT assistance and support. From Group-II banks (Private Banks), ICICI Bank tops the group by providing maximum features, IT assistance and support. HDFC, IndusInd and Kotak Mahindra Bank lag behind in this category as they provide only 24 × 7 telephonic support and FAQ/online support but not secured mail feature. From Group-III banks (Foreign Banks), Standard Chartered Bank (SCB) tops the category by providing maximum services in this category while HSBC, Citibank and American Express Bank are the followers as they are providing comparatively lesser services as compared to the leader Standard Chartered Bank.

Category 3 : Software and System Requirements

No bank is found to be providing free antivirus or antispyware software/ tool. During the study, we have found that HSBC Canada is offering free of cost antivirus software on their website (www.hsbc.ca) known as "Trusteer Rapport". However, no such software is available on India's HSBC website. This software provides additional security measures like locking the session between user browser and bank website and checks whether customer is accessing a genuine website.

Majority of banks are found to be compatible with a number of popular browsers while no information about compatible browser is displayed by UCO and Citibank. Information about compatible browsers can increase bank's web flexibility. Information related to browser settings (java, cookies settings) is being provided by the five banks (SBI, BOB, ICICI, AEB and HSBC) while no such information is displayed on the websites of remaining seven banks. Such information may increase flexibility as well as security for the customers and is in the best interests of the bank. Recommended optimal screen resolution is not provided on the websites of six banks (PNB, ICICI, Kotak Mahindra, SCB, AEB and Citibank) while other banks are providing information about the optimal screen resolution.

Under the Category 3 i.e. Software and System Requirements, SBI tops the Group-I by providing maximum information on software and system requirements, followed by BOB, UCO Bank and in the last comes PNB. ICICI and HDFC banks again top in their Group (Private Banks) by providing maximum information in this category. It is followed by Kotak Mahindra Bank which is providing information on six different sub categories. Last position is taken by IndusInd Bank in this category. From Group-III banks (Foreign Banks), HSBC tops the category by providing maximum information in this security category while Standard Chartered Bank comes in the second position here. The third position is taken by American Express

Bank and on the last Citibank is there.

Category 4 : Bank Site Authentication Technology

We have found that majority of the banks are deploying 128-bit SSL encryption and only SBI and SCB are using superior 256-bit SSL encryption technology. No information is being provided by AEB regarding bits in SSL encryption. On the other hand, 6 banks (SBI, BOB, PNB, HDFC, Indusind, Citibank) have validation certificate by "VeriSign" while 2 banks (ICICI and Kotak Mahindra) have validation certificate from "Entrust' while no information is displayed on the websites of remaining four banks.

Under Category 4 concerning bank site authentication technology, out of Group-I SBI tops the Group by using 256-bit SSL encryption with VeriSign certificate. However, PNB, BOB and UCO banks are all behind as they are using 128-bit SSL encryption. Similarly, all the Private Banks (Group-II Banks) are using 128-bit SSL encryption. Among Group-III banks (Foreign Banks), only Standard Chartered Bank is providing 256-bit SSL encryption while no information is provided on which type of CA they are using.

Category 5 : User Site Authentication Technology

It is found that there are only two banks (SBI and SCB) out of the selected banks which allow online banking customers to create and register their own login IDs instead of using the bank account IDs. This method provides convenience to users to easily remember the login IDs.

Two factor authentication is provided by 6 banks (SBI, PNB, ICICI, HSBC, AEB and Citibank) out of the 12 sample banks. Remaining 6 banks do not provide any information about adoption of two factor authentication technique. Two factor authentication technologies like SMS, token device, and USB digital certificate are examples of technologies which should be considered for effective internet banking transaction verification.

In terms of maximum attempts for logon, no information is provided by BOB and Citibank. Regarding input type, all the banks provide options for input through keyboard along with virtual keyboard for entering username and password. However, HSBC India has introduced a new security device for internet banking. This new security device provides a new level of convenient and efficient online banking experience. In this, the bank provides security device tokens with enhanced security features to online banking users and users are required to activate the security tokens. These security tokens are used with security device which provide additional security besides username and password authentication. This device is easy to use, portable and provides fraud protection and it provides additional layer of security. In relation to password restriction, only five banks (UCO, Kotak Mahindra, Indusind Bank, AEB and Citibank) are not providing any information and the remaining seven banks are displaying a password length requirement on their websites. A longer length along with use of special characters and alphabets provides better security and is strongly recommended.

Under the Category 5 concerning user site authentication technology, again SBI is the winner from Group-I banks as it is providing maximum options for user authentication. Second position is taken by PNB followed by BOB and UCO banks as they are not providing information about two factor authentication and transaction verification. Further, BOB does not provide information on maximum logon failure limits whereas UCO Bank is not providing information on password restriction. From Group II banks, ICICI Bank tops by providing all the information in this category. It is followed by HDFC Bank which is providing maximum security information except information on two factor authentication. Third position is taken by Kotak Mahindra Bank followed by IndusInd Bank on fourth position. From Group-III banks, HSBC is the winner. Remaining three banks share the second position.

Category 6 : Internet Banking Application Security Features

In the last category, it is found that activity log or transaction history is not provided by four banks (BOB, Kotak Mahindra, Indusind and HSBC). Furthermore, all banks have alert features such as SMS and/or email communications that automatically triggers to be sent to their internet banking customers. The provision of both activity logs and alert features is both handy and convenient which also serves the purpose of enhancing the security of the internet banking system. Further, five banks (BOB, Kotak Mahindra, Indusind, SCB and Citibank) are not providing default daily transfer limit while other six banks are providing information about the same. The availability of such information can increase information security and enhances privacy of existing and potential online banking customers. In terms of the 'automatic timeout feature' for inactivity, majority of the banks (10 in number) have this feature in place while the remaining two banks (BOB and UCO) provides no such information on their websites.

Thus, the Category 6 that contains internet banking application security features, SBI and PNB are the winners by providing all the options and information under this category. Second position is taken by UCO Bank followed by BOB. ICICI and HDFC banks top in Group-II by providing all the information in this category followed by Kotak Mahindra and IndusInd Bank which provides information only for automatic timeout. From Group-III banks, American Express Bank tops this category by providing all the information and the other remaining banks share the second position.

CONCLUSIONS AND RECOMMENDATIONS

With the ongoing process of enhancement in security technologies and mechanisms, the online banking is becoming more and more secure. The security mechanisms of the online banking need continuous attention and development as the cyber criminals try different methods for getting unauthorized access to online accounts of banking customers. By providing complete details about internet banking security features covered under the six categories (Table 3), a bank may enhance the security awareness for both existing and potential users of internet banking as well as help in the enhanced security of online payments.

The results of the present study have revealed a number of internet banking security features and parameters – 256-bit encryption with extended validation, SSL certificate, transaction verification, activity monitoring, multi-factor authentication techniques, auto logout feature, last login date and time display, account lockout and audit trails etc. The presence of all these features makes web experience of an internet banking user more safe and secure.

Most of the banks under study have generally provided a standard security system for online banking with some optional security services to their customers. However, these banks should also implement mandatory multifactor authentication techniques for logon as well as for verification of online transactions. As far as the overall rating is concerned, first position is shared by SBI and ICICI Bank as they are providing most of the information concerning security and privacy falling under all the six categories. From the Foreign Sector bank group only Citibank is lagging behind while overall UCO Bank holds the last position. Under Group-I (Public Sector Banks), SBI has emerged as clear winner by providing maximum number of services on their web portal, which is followed by PNB. On the third position, BOB is there while UCO Bank is at the last position in this group. ICICI tops in Group-II (Private Sector Banks), while HDFC is at second position which is followed by Kotak Mahindra Bank at third position and IndusInd Bank is at the last position in this group. In Group-III (Foreign Sector Banks), HSBC is at first position by providing maximum number of services under six categories. Second position has been taken by SCB while AEB and Citibank are at third and fourth position. As per the overall rating/ scoring is concerned from all the three groups, first position is shared by SBI and ICICI Bank by providing most of the information under all the six categories while UCO Bank holds the last position.

As far as recommendations are concerned, the banks should provide improved authentication mechanisms as security measures to detect and prevent online frauds. In terms of website authentication, banks need to consider upgrading from 128-bit SSL encryption to a 256-bit encryption method for enhanced security. Furthermore, upgrading from standard to extended validation SSL certificate should also be considered. These two upgrades can provide better confidentiality to both existing and potential internet banking customers. It is also important for the banks to educate and support their customers from time to time so that they gain knowledge about various security threats and risks. Further, banks should be aware of customers' feedback/concerns/demands/expectations/mistrusts by conducting a survey and offering rewards for customer feedback. The feedback from these surveys will be helpful in building the confidence of both existing and potential internet banking customers.

The banks should also consider to adopt a policy of offering compensations for losses due to any potential security threats/risks which may occur by inexperienced customers or lack of their knowledge and/or awareness. As the findings in the study reveal, not even a single bank from the selected twelve banks from different bank groups is providing free antivirus/antispyware software/tool for their customers. The banks should at least offer a useful link or special deal to download or update antivirus and internet security software and firewall protections. As a future plan, the banks should consider deploying biological authentication techniques like retina scan, finger scan, face recognition, voice recognition etc. to protect their online banking systems against the attackers.

By implementing the above discussed recommendations in their online banking systems, the banks can standardize information privacy/security and usability for their customers. Finally, the effectiveness of this study can be further enhanced by conducting an in-depth customer interview and audit on the structure and design of the banking websites.

References

Aladwani, M. (2001), Online Banking : A Field Study of Drivers, Development Challenges and Expectations, *International Journal of Information Management,* 213-225.

Al-Somali, S. A.; Gholami, R.; and Clegg, B. (2008), Internet Banking Acceptance in the Context of Developing Countries : An Extension of the Technology Acceptance Model (Operations & Information Management Group, Aston Business School, Birmingham B47ET, UK).

Bauer, H.; Hammerschmidt, M.; and Falk, T. (2005), "Measuring the Quality of E-banking Portals," *International Journal of Bank Marketing*, Vol. 23, No. 2, pp. 153-175.

Fitzergelad, K. (2004), An Investigation into People's Perceptions of Online Banking. Accessed online at: http://staffweb.itsligo.ie/staff/eward/ebus%200203/Discussion%20topics/Online%20Banking.htm

Gartner (2005), Online Survey Report "Phishing Attack Victims Likely Targets for Identity Theft" Accessed online at https://www.gartner.com/doc/431660?ref=SiteSearch&sthkw=Consumer%20Trust%20in%20Online%20Commerce&fnl=search, January 2014

Grethen, H. (2001), 'The E-banking Revolution', Speech Delivered at the Luxembourg International Trade Fairs.

HSBC Canada, Accessed online at http://www.hsbc.ca/1/2/personal/security/free-downloads, February 2014.

Jayaraman, M.; and Ernest C. D.R. (2012), Adoption of Retail Internet Banking : A Study of Demographic Factor, *Journal of Internet Banking and Commerce,* December 2012, Vol. 17, No. 3.

Kalakota, R.; and Whinston, A. B. (1997), Electronic Commerce : A Manager Guide, Addison-Wesley.

Kaur, R. (2012), "An Impact of IT on Branch Productivity of Indian Banking in the Era of Transformation".

Kesharwani, A.; and Radhakrishna, G. (2013), Drivers and Inhibitors of Internet Banking Adoption in India, *Journal of internet Banking and Commerce,* December 2013, Vol. 18, No.3.

Liao, Z.; and Cheung, M. (2003), Challenges to Internet E-Banking, *Communications of the ACM* (http://www.acm.org/cacm), Vol. 46 No.12, pp. 248-250.

Malhotra, P.; and Singh, B. (2009), Analysis of Internet Banking Offerings and Its Determinants in India, *Internet Research,* Vol.20 No.1, pp. 87-106.

Mukti, N. (2000), Barriers to Putting Businesses on the Internet in Malaysia, *The Electronic Journal of Information Systems in Developing Countries,* Vol. 2 No.6, pp. 1-6.

RSA (2005), Online Report, 'The True Cost of Protecting Customers Online Accounts' Accessed Online February, 2014 at https://rsasecurity1.rsc03.net/servlet/campaignrespondent

RSA Security (2005), Online Report, "Consumer Study Reveals Major Concerns Over Online Security and Identity Protection" accessed online at http://www.rsasecurity.com/press_release.asp? doc_id=5522&id=1034, February, 2014.

Reserve Bank Of India (2011), Accessed online at http://www.rbi.org.in/scripts/BS_PressReleaseDisplay.aspx?prid=23789, on January 2014.

Rossignoli, C.; and Zardini, A. (2013), "When Customer Behaviours Change, Should Banks'

Approaches to Online Trading Stay the Same?", *Journal of Internet Banking and Commerce*, August, Vol. 18, No. 2.

Sathye, M. (1999), Adoption of Internet Banking by Australian Consumers : An Empirical Investigation, *International Journal of Bank Marketing*, Vol. 17 No.7, pp. 324-34.

Symantec Corporation White Paper, (2005), "Symantec Security Response" Accessed online at http://www.symantec.com/index.jsp.

Usman, Ahmad K.; and Shah, Mahmood H. (2013), Critical Success Factors For Preventing E-Banking Fraud, *Journal of internet Banking and Commerce,* August 2013, Vol. 18, No.2

Watchfire Corporation (2005), Online Survey, "Privacy of Online Banking Key to Customer Loyalty : 2005 Privacy Trust Survey for Online Banking Links Consumers' Perception of Trust in their Banks to Confidence in Banking Online" accessed online at http://www.businesswire.com/news/home/20050405005619/en/Privacy-Online-Banking-Key-Customer-Loyalty-2005#.Uzep4qhmOSo.

White, H.; and Nteli, F. (2004), Internet Banking in the UK : Why Are There Not More Customers? *Journal of Financial Services Marketing,* Vol. 9 No. 1, pp. 49-56.

Approaches to Online Banking [illegible] The Case [illegible]", Journal of Internet Banking and Commerce, August, Vol. 10, No. 2.

Sathye, M. (1999), Adoption of Internet Banking by Australian consumers: An Empirical Investigation, International Journal of Bank Marketing, Vol. 17, No. 7, pp. 324-334.

[illegible] Commission White Paper (2001) "[illegible]" [illegible] [illegible]

[illegible] and [illegible] (2013) [illegible] E-Banking in India [illegible] Vol. 19, No. 1.

[illegible] (2005) Online [illegible] Review of Online Banking [illegible] 2005 Online Trust Survey for Online Banking [illegible] Division of Finance and Commerce [illegible] [illegible]

[illegible] (2005) Internet Banking in [illegible] Journal of Financial Services Marketing, Vol. 9, No. 3, pp. [illegible]