Indian Management Studies Journal 20 (2016) 21-37

Indian
Management
Studies Journal

E-Banking Security and Bank Customers' Discernment : An Empirical Investigation

Dhiraj Sharma* and Tejinder Pal Singh Brar**

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

*** Department of Computer Science, Apeejay College of Fine Arts, Jalandhar*

Abstract

The Internet has played a vital role in changing how we interact and do business today. E-commerce allows businesses to interact with their customers in more time and cost effective manner. Banking industry is one such industry that is using new e-channels to effectively reach to its customers. The electronic banking systems promises a number of advantages. However, the challenges that oppose E-banking are the bank customers' concerns of security and privacy of information and transactions. This exploratory study is an effort to examine the factors affecting bank customers' perspective towards current E-banking security status. It has been found that bank retail customers have increased concerns about secure transactions and the results indicated that the intention to use online banking is positively affected primarily by security and privacy concerns. Despite the growth in the usage of e-banking channels and banking technologies, retail customers' still avoid transacting through E-channels due to the perceived insecure and vulnerable environment.

Key Words

Bank retail customer, Security, E-banking, Trust

INTRODUCTION

Adoption and usage of E-banking depends upon a number of factors like secure online environment, privacy, trust and even the perceived stress from using technology known as 'Technostress' [Liao and Cheung (2002); Mukti (2000); Sharma and Gill (2015)]. Malhotra and Singh (2009) mentioned that despite concerns

about security and privacy of transactions, slowly but steadily the Indian customer is moving towards Internet banking. Customers have apprehension about the security of the system, in particular with the unwarranted access to their accounts and secrecy of their personal information, [Brar *et al.* (2015)]. In a survey conducted by White and Nteli (2004) found that UK customers ranked the security of the bank's website as the most important attribute of Internet banking service quality. This situation is further illustrated by Sathye (1999), who found that security concerns and lack of awareness about the Internet banking was the two obstacles for the non-adoption of E-banking.

Changes in threat landscape have been reported by online security experts. This is because attackers have developed more complicated methods to compromise authentication mechanisms and gain unauthorized access to customers' information. According to [Jarvenpaa *et al.* (2000); Ponemon (2005)] technology-related variables are as important as traditional factors in predicting customer's behavior in online environment. Moreover, perceptions of E-banking security have direct influence on trust and usefulness and indirectly affect ease of use. Nevertheless, trust in the banking sector has not yet been fully translated in the electronic world. Trust is difficult to achieve without in person interaction, and it's a matter of debate that whether artificial agents are capable of trusting and/ or being trusted, [Yousafzai *et al.* (2009); Pieters (2010); Avizienis *et al.* (2004)]. The more a user trusted the bank and its website, the higher their belief that online banking was easy. Higher levels of security may also make online banking more useful, [Alnsour and Al-hyari (2011); Friedman *et al.* (2000); Gefen *et al.* (2003)].

Customers have not adopted B2C e-commerce in the same way primarily because of risk and trust related issues [Yousafzai *et al.* (2003); Grewal *et al.* (2004); Avizienis *et al.* (2004)]. Number of authors argued that banking and finance sector is probably the most advanced sector in adopting defensive measures but despite ongoing security efforts, it remains vulnerable to a variety of events [Goetz (2003); Dapp (2012); Chickowski (2006); Klein (2007); Aladwani (2001); Bradley and Stewart (2003)]. Goetz E. (2003) examined the Internet banking vulnerabilities and concludes that banking industry faces a multitude of physical and cyber threats from criminals, hackers and malicious insiders.

Several studies offered solutions and recommendations for safe E-banking like Alsajjan and Dennis (2006) advised banks should publicly advertise the safety and informative issues rather than building brand awareness. Similarly, Infosys (2010) insisted on implementation of mandatory and strong controls on the access and monitoring of sensitive data. Outsourcing of various banking

activities and increasing concerns over insider and outsider threats in banks puts pressure on the need of enhanced security. [Bala and Norita (2011); Viega and McGraw (2001)] suggests developers have to incorporate security during the development process itself in order to produce software assurance systems, since the existence of flaws in the design or coding stage of the development process can open web applications to a wide range of attacks. Fatima (2011) suggests that banks must be more responsive to security requirements while Dandash *et al.* (2008) on the other hand, proposed an efficient new scheme which can prevent fraud by applying different security algorithms, generating and updating limited-use secret keys. It uses advanced authentication technologies and is well adapted to any possible future technology.

Now a day's data breaches are happening all over the world regularly [Dinesh (2011); Kitten (2014); Schwartz (2014); Karimi (2014); Finkle and Henry (2013)]. Many data breaches are linked to compromised usernames, passwords and OTPs. It raises a question: why do not we make strong security controls? Infact, there is no particular security solution to defend against today's versatile attacks. In spite of innovation in security technologies, attackers still manage to breach banks' resistance from time to time [Kumar (2014); Tripathy (2014)]. While analyzing Indian scenario Bipindra (2014) mentioned Defense Research and Development Organization's (DRDO) computers were hacked by Chinese hackers and carted away electronic files relating to Cabinet Committee on Security (CCS). While taking note on the state-wise scenario in India, NCRB (2013) reported 4,356 cases were registered under IT Act during the year 2013 as compared to 2,876 cases during 2012, thus showing an increase of 51.5% in 2013 over 2012. Similarly, according to Gurung (2014) there is an increase in the cyber crime by 51%. As more and more people are exposed to the information superhighway, privacy and security goes hand and hand and this is crucial for the growth of electronic banks. Brar *et al.* (2013) suggest that trust and perceived risks are direct antecedents of intention to use E-banking. This means if a customer has no trust on e-banking then he will not prefer e-channels for conducting transactions.

RESEARCH OBJECTIVES AND METHODOLOGY

The primary objective of this research study is to examine bank retail customers' perceptions regarding trust, privacy and security in electronic banking environment and to study the customers' perceptions about E-banking service quality. For the purpose of data collection a structured questionnaire was prepared and distributed among 200 bank retail customers' sample taken randomly from the four major commercial banks (two private and two foreign sector banks) from

Chandigarh and Mohali. Only those bank retail customers were interviewed who were using e-banking services for the last one year at least. Out of a sample of 200 bank customers, only 178 questionnaires were found to be complete and worthy of analysis.

SERVICE QUALITY LEVEL OF E-BANKING SERVICES

In this section factor analysis technique was applied on respondents' responses with regard to six service quality variables (Empathy, Security, Privacy, Responsiveness, Reliability and Tangibility) related E-banking service quality levels. The respondents were required to rate statements, which ranged from strongly disagree to strongly agree. For this purpose, the following null hypothesis (H_{01}) was formulated.

H_{01} : There is no association between perceived E-banking security of transactions and customer satisfaction levels

Scale Development

A scale was developed to identify the service quality regarding E-banking services provided by bank. Total 21 variables were selected to find the service quality E-banking services (refer Table 1).

Table 1
Selected Service Quality Variables

Reliability	
RLB-1	Bank provides relevant and accurate information
	E-banking website links are problem-free
	Bank restricts unauthorized access
	Bank shows a sincere interest to solving the problem
RLB-2	Web site provides a confirmation of the service
	I rely my principal bank
	Bank performs online services in right manner
RLB-3	Bank provides online services at the time it promises
	Bank insists on error-free records
	Bank website does not freeze
	Information on bank's website is constantly updated
RLB-4	Processing of transactions is error free
	Bank provides wide range of products and services
	I can rely on the web pages functioning

Contd. Table 1

RLB-5	Information content and texts are easy to understand
	The bank's website does not use cookies
Responsiveness	
RSP-1	Bank is willing to help customers
	Through E-banking customers can immediately connect to bank accounts
	Instant help for problems/queries
	Websites provides options for complaints, pinions and request services.
RSP-2	Customers are able to get on the site quickly
	It is easy to find what I need on the website
	Quick to complete a transaction
	Bank's website doesn't require lot of effort
RSP-3	Structure of online content is easy to follow
	Bank is willing to provide prompt service to customers.
	Bank gives prompt responses to the requests by e-mail or other means.
RSP-4	The home page of the site motivates me to continue browsing.
	The response from e-banking to their customer is faster
RSP-5	The Internet banking can be relied to solve the banking problems quickly
	Bank's website has online customer service representatives
Tangibles	
TAN-1	Our bank has up-to-date equipment & technology
	E-banking website is visually appealing
	It is easy to find information on bank's website
	E-banking web site is easy to use and navigate
TAN-2	The website is available in the language one can understand.
	There is clear, simple and understandable guidance provided on website
	Ergonomic visual structure and design are important for using E-banking
	Graphical user interface is also considered as an important determinant
Empathy	
ETH-1	Bank understand specific needs of the customer
	Bank gives the individual attention
	Help desks or call centers of online bank gives personal attention
ETH-2	Operating hours of banks help desks are convenient for customers
	Bank understand specific needs of customer
ETH-3	Bank has best interest at heart
	Speed of E-transactions flow is critical to user satisfaction

Contd. Table 1

Privacy	
PRV-1	Customers' financial information may not be passed on to other organizations
	E-banks ensure protection of personal information, risk of financial loss
	Privacy factor influences the adoption of E-banking services in India
PRV-2	The bank's website is secure for giving financial information
	There are privacy policies in Internet banking
	There are guarantees of Internet banking
PRV-3	I feel safe using Internet banking
	Bank can be relied upon to keep their promises and service pledge
Security	
SEC-1	Security is prime factor for adoption of E-banking services
	Misuse of personal information.
	Internet hackers may take control of customer account
	E-banks will compensate for any losses due to security or infringement
	It is harmless to do transactions with the Internet banking
SEC-2	I'll be loyal with Internet banking because I found this service as secure
	I find it necessary to be cautious in dealing with my bank
	For banks security is the most important issue
SEC-3	Banking infrastructure is reliable in correcting erroneous transactions
	Satisfaction with the security system of the e-banking

Source : Developed by the Researchers

Scale Refinement

Item wise reliability analysis was executed on selected variables for developing a reliable scale.

For the determination of reliability assessment of uni-dimensionality, reliability and validity have been answered. Hence, based upon these concepts the scale generated for present objective was refined and purified. Also the inter-item correlations and Cronbach's alpha statistics were employed to conduct the scale reliability analysis and to know extend to which items were correlated with the remaining items in a set of items under consideration. The results are shown in Table 1.1. The value of Cronbach's alpha coefficient of 0.6 and above is good for research in social science [Cronbach, (1990)] also the corrected-item-total correlation > 0.5 and inter-item correlation is more than 0.3. It is likewise important to mention that corrected-item-total correlation > 0.5 and inter-item correlation >0.3 is good enough for reliability of the scale [Hair *et al.*, (2009)]. Here it is

Table 2

Table Scale Reliability Analysis

Variables	Initial	Extraction	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted	Mean	Std. Dev.
ETH-1	1.000	.575	.542	.910	3.05	.944
ETH-2	1.000	.622	.557	.936	3.17	.912
ETH-3	1.000	.526	.500	.949	3.22	.883
SEC-1	`1.000	.575	.559	.932	3.10	.887
SEC-2	1.000	.716	.575	.915	3.11	.960
SEC-3	1.000	.767	.512	.933	3.30	.987
PRV-1	1.000	.782	.512	.952	3.26	1.043
PRV-2	1.000	.822	.516	.941	3.23	.997
PRV-3	1.000	.720	.605	.896	3.16	1.064
RLB-1	1.000	.619	.616	.822	3.19	.923
RLB-2	1.000	.654	.545	.895	3.39	1.054
RLB-3	1.000	.709	.572	.905	3.28	.968
RLB-4	1.000	.750	.607	.944	3.33	1.052
RLB-5	1.000	.802	.573	.964	3.10	.922
RSPN-1	1.000	.813	.567	.919	3.15	.965
RSPN-2	1.000	.794	.539	.875	2.86	.913
RSPN-3	1.000	.776	.508	.931	2.84	.959
RSPN-4	1.000	.750	.548	.907	3.01	.935
RSPN-5	1.000	.818	.540	.874	2.92	.949
TANG-1	1.000	.778	.551	.942	2.98	.938
TANG-2	1.000	.799	.570	.876	2.97	.932
Item Means : Mean = 3.125, Minimum = 2.482, Maximum = 3.393, Range = .551, Max/Min = 1.194, Variance = .023, N = 21						

Source : Developed by the Researchers

pertinent to mention that commonality >0.5 is sufficient for the explanation of constructs [Hair *et al.* (2009)]. All these values show factors analysis has extracted good quantity of variance in the items.

RESULTS AND DISCUSSION

Principal component analysis (PCA) was conducted as a means of data reduction, to ascertain if the face validity of the items held [Pallant (2001)]. Prior to performing PCA the suitability of data for factor analysis was assessed. The correlation matrix revealed many coefficients of .3 and above. PCA revealed the presence of 21 components with Eigen values exceeding 1. Factor loadings represent how much a factor explains a variable in factor analysis. Loadings can range from -1 to 1. Loadings close to -1 or 1 signify that the factor strongly affects the variable. Loadings close to zero indicate that the factor has a weak influence on the variable. Table 1.2 shows extracted factor along with their description regarding overall impact.

Table 3
Descriptions of Extracted Factors

Factor	Description
ETH-1	Statement "bank understand customer needs" has highest factor loading of .886 in ETH-1 while statement "personal attention by bank personnel" show low factor loading of .822. This shows less overall impact in factor ETH-1.
ETH-2	In this factor statement "Convenient operating hours" has strong impact (.895) in ETH-2 while "Bank understand customer's specific needs" has comparatively less impact because of its low value of factor loading (.873).
ETH-3	This factor was developed from two variables i.e. "best has best interest at heart" with factor loading of (.820) and "satisfaction with speed of e-transactions" with factor loading of (.738). It covers 1.401 of the Eigen values.
SEC-1	This factor includes five variables i.e. "prime factor", "misuse of information", "control of customer account", "loss compensation" and "safe transactions". The factor loading ranges from .788 to .880 with highest factor loading of .880 for "Security as prime factor" and lowest factor loading of .788 for "Safe transactions".
SEC-2	This factor was developed from three variables; i.e., "loyalty and trust", "satisfaction with security system" and "security as main issue". Loyalty and trust in E-banking has highest factor loading of .876 whereas "satisfaction with security system" show lowest factor loading of .850.

Contd. Table 3

SEC-3	This factor was developed from two variables "security issue" and "erroneous transactions" with highest factor loading of .827 for "security issue" and lowest factor loading for "Erroneous transactions".
PRV-1	It includes four variables i.e. "Financial information may not be passed on", "risk of frauds and financial loss" and "influence of privacy" with highest factor loading for "financial information may not be passed on" and lowest factor loading for "privacy factor influences the adoption".
PRV-2	This factor includes "secure financial information on website" which has the lowest factor loading (.813) and highest factor loading for "privacy policies" (.889).
PRV-3	This factor was developed from two variables i.e. "safe internet banking" with highest factor loading of .882 and lowest factor loading (.877) for "promise and service pledge".
RLB-1	It includes four variables "relevant and accurate information" with highest factor loading of .958, "accurate links", "restrict unauthorized access" and "interest in problem solving" with lowest factor loading of .751.
RLB-2	This factor was developed from three variables i.e. "confirmation of service" with highest factor loading (.823), "trust on principal bank" and lowest factor loading (.799) for "performing E-services in right manner".
RLB-3	It includes four variables i.e. "bank provides online services" (highest factor loading), "error free records", "website freeze", and "constant updated information" (lowest factor loading).
RLB-4	This factor was developed from another three variables i.e. "error free transactions" which has highest factor loading of .884, "wide range of products" and "reliable web page functioning" with lowest factor loading of .777.
RLB-5	This factor was developed from two variables "information content" and "use of cookies". Information content is easy to understand has highest factor loading of .895 while Website does not use cookies has lowest factor loading of .880.
RSPN-1	It includes four variables "willingness to help customers" with highest factor loading of .946, "connect to bank accounts", "help for problems" and "provision for complaints, opinions and services" (lowest factor loading of .748).

Contd. Table 3

RSPN-2	This factor was developed from four variables i.e. "quick access to website", "easy to find contents", "quick to complete transaction" and "website does not require lot of effort". Quick access to website had highest factor loading whereas website does not require lot of efforts has lowest factor loading.
RSPN-3	It includes three variables i.e. "structure of online content" with highest factor loading of .899 and lowest factor loading of .791 for "willingness to provide prompt service" whereas factor loading of .791 for "prompt response to customer request".
RSPN-4	It covers 1.709 of the Eigen values. This factor was developed from another two variables i.e. "continue browsing" with highest factor loading and "factor response" with lowest factor loading.
RSPN-5	This factor was developed from two variables "quickly solving problems' with highest factor loading and "customer service" with lowest factor loading.
TANG-1	This factor was developed from four variables i.e. "up-to -date technology" with highest factor loading of .923, "visual appeal", "easy to find information" and lowest factor loading for "website easy to navigate and use".
TANG-2	It includes four variables "understandable language" with highest factor loading (.813), "clear and simple guidance", "visual structure" and "graphical user interface" with lowest factor loading (.698).

Source : Developed by the Researchers

Table 1.3 shows the factor analysis of different variables and analysis of extracted factors from these variables. Each component was defined by at least three scale items. Kaiser-Meyer-Olkin (KMO) Measure of Sampling Adequacy (MSA) values are sufficient enough for validating factor analysis results. Here, it is pertinent to mention that KMO>0.6 and P<0.5 are good enough for research in social sciences [Hair *et al.*, (2009)]. The Bartlett's Test of Sphericity also has a significant value, i.e. (p<0.5). All these requirements are sufficient for validating factor analysis.

Table 4

Table Showing Variance and Eigen Values of Different Factors

Factor Number	Factor	Variance Values	Eigen	Highest Factor Loading	Lowest Factor Loading
First	ETH-1	49.507%	5.446	.886	.822
Second	ETH-2	16.269%	1.790	.895	.873
Third	ETH-3	12.733%	1.401	.820	.738
Fourth	SEC-1	47.507%	7.541	.788	.880
Fifth	SEC-2	16.269%	2.790	.850	.876
Sixth	SEC-3	12.672 %	1.921	.827	.811
Seventh	PRV-1	47.650%	5.057	.861	.980
Eight	PRV-2	16.061%	1.423	.818	.889
Ninth	PRV-3	12.442%	1.913	.877	.882
Tenth	RLB-1	37.422%	7.702	.751	.958
Eleven	RLB-2	11.157%	2.897	.799	.823
Twelve	RLB-3	9.512%	1.817	.766	.895
Thirteen	RLB-4	6.564%	1.716	.777	.884
Fourteen	RLB-5	6.123%	1.241	.880	.895
Fifteen	RSPN-1	37.401%	7.711	.946	.748
Sixteen	RSPN-2	11.150%	2.880	.884	.789
Seventeen	RSPN-3	9.520%	1.820	.899	.780
Eighteen	RSPN-4	6.508%	1.709	.770	.766
Nineteen	RSPN-5	6.129%	1.252	.882	.898
Twenty	TANG-1	32.414%	6.982	.923	.821
Twenty one	TANG-2	12.101%	3.921	.923	.698

Source : Developed by the Researchers

Correlations of all variables with each other were examined using Pearson Correlation coefficients. Correlations among different items were quite satisfactory and were also significant. According to the scale used if all the 21 items get a rating of 5 each, the total score would be 105. There is a sufficient correlation to go ahead with factor analysis.

Table 5
KMO, Bartlett's Test of Spericity, Load and Eigen Values

	Empathy	Security	Privacy	Reliability	Respon-siveness	Tangibles
Cronbach's alpha	.796	.721	.805	.973	.906	.983
KMO	.960	.880	.860	.855	.867	.879
Bartlett's test of spericity	X^2 = 4351.011 DF=55	X^2 = 7221.026 DF=53	X^2 = 9621.027 DF=55	X^2 = 6729.971 DF=136	X^2 = 6731.89 DF=139	X^2 = 6730.811 DF=57
Load values	.738 to .895	.788 to .880	.813 to .980	.751 to .958	.748 to .946	.698 to .923
Eigen values	1.401 to 5.446	1.921 to 7.446	1.913 to 5.057	1.241 to 7.702	1.252 to 7.711	3.921 to 6.982

Source : Developed By the Researchers

Factor analysis is performed with varimax rotated, Principal Component Analysis. The scale reliability has also made for factors, so classified. Each component was defined by at least three scale items. The 21 factors classified using the factor analysis is presented in the above tables having loads more than 0.5 are considered good. Items with factor loadings <0.5 were removed. Table 1.4 shows different ranges of KMO, Bartlett's test of Spericity, Load values and Eigen values of SERVQUAL variables.

Table 1.5 shows variables with dominant path loading. After analyzing the data it is clear that customers termed security as prime factor and they are increasingly worried about hacking of their accounts and misuse of their personal information by the attackers. Moreover, it has been found that no compensation is expected by customers in case they face online attack. Regarding privacy of their account, customers do not feel safe while transacting through E-banks. Banks kept their promises by introducing new safety measures but these measures are far from effective in countering latest online threats. The H01 hypothesis has been rejected as the extracted factors have significant path loading to indicate the satisfaction level of a customer; hence besides other service quality variables security have significant association to frame satisfaction level towards the online services provided by bank. This section helped us in understanding the online

Table 6
Dominant Factors

Service Quality Variable	Factors
Empathy (ETH-1)	Bank understand customer needs; Bank gives the individual attention; Help desks or call centers gives personal attention
Security (SEC-1)	Security is prime factor for E-banking services; Misuse of personal information; Internet hackers may take control; No compensation for any losses; It is harmless to do transactions
Privacy (PRV-3)	Feeling of safety while using E-banking; Bank keep their promises
Reliability (RLB-1)	Relevant and accurate information; Problem-free and accurate web-links; Restriction of unauthorized access; Interest to problem solving
Responsi-veness (RSP-2)	Customers get on to the site quickly; Easy to find the information on the website; Quick to complete a transaction; Website doesn't require lot of effort
Tangibility (TAN-1)	Up-to-date equipment & technology; Website is visually appealing; Easy to find information on bank's website; Website is easy to use and navigate

Source : Developed By the Researchers

banking service quality in E-banking and the items which are playing more and less important role towards the satisfaction of respondents for the online services provided by bank.

CONCLUSIONS AND RECOMMENDATIONS

In principle, any activity that carries some risks with it on a customer's computer system is a candidate for strong authentication. The interesting concept emerging from current E-banking scenario is the need for layered security. Strong authentication is required at different levels of conducting the transactions via E-channels. Banks need to realign their authentication infrastructures to include a mix of multi factor authentication measures. It is important not only to evaluate E-banking applications and identify existing vulnerabilities but also to assess layered security approaches, and the areas where these additional layers of authentication should be added.

Despite the growth in utilization of the Internet and Internet banking technologies, retail customers' still avoid transacting through E-channels due to insecure environment and exposure to various online threats. Past studies show concerns over security and trust that constitute an obstacle in the adoption of E-banking. This study investigated various security-related aspects also from customer's perspective. It has been found that majority of customers think that besides updates and protection of their information; they still have fears related to online threats and financial losses. Banks should approach security considerations as part of their service offerings. An effective authentication method should have customer acceptance, reliable performance, scalability to accommodate growth, and interoperability with existing systems and future plans. The level of authentication used by the financial institutions should be appropriate to the risks associated with those products and services.

References

Aladwani, M. (2001), Online banking: a field study of drivers, development challenges, and expectations. *International Journal of Information Management*, pp. 213-225.

Alnsour, M.; and AL-hyari, K. (2011), Internet Banking and Jordanian Corporate Customers : issues of security and trust, *Journal of Internet Banking and Commerce,* Vol. 16, No.1. Available at: http://www.arraydev.com/commerce/jibc.

Alsajjan, B. A.; and Dennis, C. (2006), The Impact of Trust on Acceptance of online banking, *European Association of Education and Research in Commercial Distribution*, 27-30 June 2006. Brunel University – West London, United Kingdom.

Avizienis, A.; Laprie, J.; Randell, B.; and Landwehr, C. (2004), Basic Concepts and Taxonomy of Dependable and Secure Computing, *IEEE Transactions on Dependable and Secure Computing*, 1(1), 11–33.

Bala, M. S.; and Norita, M. N. (2011), Secure E-commerce Web Development Framework, *Information Technology Journal*, 10(4) : 769–779.

Bipindra, N. C. (2013), *Chinese 'hack' DRDO computers,* Retrieved online at http://www.newindianexpress.com/nation/article1500336.ece

Bradley, L.; and Stewart, K. (2003), A Delphi Study of Internet Banking, *Marketing Intelligence and Planning*, 21 (5), 272-281.

Brar, T. P. S.; Sharma, D.; and Khurmi, S. (2013), Influence of Trust in Espousal of E-Banking in India, *International Journal of Research in Electronics and Computer*

Engineering, IJRECE Vol. 1 Issue 1 Oct-Dec 2013.

Brar, T. P. S.; Sharma, D.; and Khurmi, S. (2015), Impact of Online Threats on Usage of E-Banking, *The Research Journal (TRJ)*, TRJ Vol. 1 Issue 1 May-June 2015.

Chickowski, E. (2006), *Web Security Fears Cause $2 billion online commerce loss in 2006*, SC Magazine, Available at: http://haymarket.ec-messenger.com/re?l=1hmb1qIfvmdmdIe.

Dandash, O.; Wang, Y.; Le, P. D.; and Srinivasan, B. (2008), Fraudulent Internet Banking Payments Prevention using Dynamic Key, *Journal of Networks*, Vol. 3, No. 1.

Dapp, T. F. (2012), Online Article "Growing need for security in online banking, biometrics enjoy remarkable degree of acceptance", *Banking and Technology Snapshot Digital Economy and Structural Change,* Deutsche Bank, Available at : www.dbresearch.com

Dinesh, T. C. (2011), *What the Future of Online Banking Authentication Could Be,* Available at: www.infosys.com/finacle.

Fatima, A. (2011), *E-Banking security issues – Is there a solution in biometrics? Journal of internet Banking and Commerce,* August 2011, Vol. 16, No.2. Available at: http://www.arraydev.com/commerce/jibc/

Finkle, J.; and Henry D. (2013), *Target hackers stole encrypted bank PINs,* Available at http://www.reuters.com/article/2013/12/24/us-target-databreach-idUSBRE9BN0L220131224.

Fitzergelad, K. (2004), An Investigation into people's perceptions of online banking, Available at : http://staffweb.itsligo.ie/staff/eward/ebus%200203/Discussion% 20topics/Online% 20Banking.ht.

Friedman, B.; Kahn, P.; and and Howe, D. (2000), Trust Online, Communications of the ACM 2000; 43 : 34-40.

Gefen, D.; Karahanna, E.; and Straub, D. W. (2003), Inexperience and experience with online stores : The importance of TAM and trust, *IEEE Transactions on Engineering Management*, 50(3), 307-321.

Goetz, E. (2003), Survey and Analysis of Security Issues in the U.S. Banking and Finance Sector, Available at : www.ists.dartmouth.edu

Grewal D.; Iyer G.; and Levy M. (2004), Internet Retailing : Enablers, Limiters and Market Consequences*, Journal of Business Research*, 57(7), pp. 703-7013.

Gurung, V. (2014), Latest Cyber Crime Reports of India, Available at http://www.cyberkendra.com/2014/07/latest-cyber-crime-reports-ofindia.html#.U_aF_8WSySo

Infosys (2010), FINACLE strengthens data security using oracle database vault, audit vault and advanced security, Available at: http://www.infosys.com/finacle/

Jarvenpaa, S. L.; Tractinsky, N.; and Vitale, M. (2000), Customer Trust in An Internet Store, *Information Technology and Management*, 1, 45-71.

Karimi, S. (2014), 6 Things You Must Do After Hackers Steal Your Credit Card Data, Retrieved online at http://money.usnews.com/money/blogs/my-money/2014/02/19/6-things-you-must-do-after-hackers-steal-your-credit-card-data.

Keffala, M. (2010), Barriers to the Adoption and the Usage of internet banking by Tunisian Customers, Available at : http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1566719.

Kitten (2014), How to Improve Threat Detection, Available at: http://www.bankinfosecurity.com/interviews/banks-how-to-improve-threat-detection-i-2328

Klein, A. (2007), The new front line in defending against online threats, *E-Commerce Times,* Available at : http://www.technewsworld.com/rsstory/55686.html

Kumar, V. (2008), Alternative Perspectives on Service Quality and Customer Satisfaction : The Role of BPM, *International Journal of Service Industry Management*, Vol. 19 No. 2, pp. 176-187, 2008.

Kumar, V. (2014), *Cyber snoops hack India's secrets : Report reveals how internet spies may have 'compromised' the nation's securit*y. Available at http://www.dailymail.co.uk/indiahome/indianews/article-2586442/Cyber-snoops-hack-Indias-secrets-Report-reveals-internet-spies-compromised-nations-security.html#ixzz3B5sPlTfV.

Liao, Z.; and Cheung, M. T. (2002), Internet Based E-banking and Customer Attitudes : An Empirical Study, *Information and Management*, 39, 283–295.

Malhotra, P.; and Singh, B. (2009), Analysis of internet banking offerings and its determinants in India. *Internet Research*, 20 (1), 87-106.

McAfee, Inc. (2007), *Online identity theft trends.* Available at: http://www.mcafee.com/us/about/press/corporate/2007/20070115_182020_r.html.

Mukti, N. (2000), Barriers to Putting Businesses on the Internet in Malaysia, *The Electronic Journal of Information Systems in Developing Countries*, 2(6), 1-6.

NCRB (2013), Cyber Crimes, Available at : http://ncrb.gov.in/CD-CII2013/Home.asp

Pieters, W. (2010), *Explanation and trust : what to tell the user in security and AI?* Published with open access at Springerlink.com

Ponemon (2005), *Privacy Trust Survey for Online Banking*, Available at : http://www.watchfire.com/news/whitepapers.aspx#finserv

Qiu, X. L. (2008), Chinese Customers' Banking Habits and E-banking Barriers, *International Journal of Business and Management,* Vol. 3, No. 2.

Sathye, M. (1999), Adoption of Internet Banking by Australian Customer : An Empirical Investigation, *International Journal of Bank*, Vol. 17 (7), 324-334.

Schwartz, M. J. (2014), *UPS Reveals Data Breach,* Available at www.bankinfosecurity.com/ups-reveals-data-breach-a-7217

Shalhoub, K. Z. (2002), *Trust and loyalty in electronic commerce : An Agency Theory Perspective*, Quorum Publishing, New York, NY.

Sharma, D.; and Gill, T. K. (2015), Is Technology Stressful? (A Study of Indian Public Sector Banks), *International Journal of Computer Science and Technology,* Vol. 6, Issue 1, 2015.

Stewart, K. J. (1999), *Transference as a means of building trust in World Wide Web sites*, Proceedings of the 20th International Conference on Information Systems, pp. 459–464.

Tripathy, D. (2014), India-probes-media-report-of-Huawei-hacking-BSNL, Retrieved online at http://www.livemint.com/Industry/rAWayE115erqLzGZOXxVDO/India-probes-media-report-of-Huawei-hacking-BSNL.html.

Viega, J.; and McGraw, G. (2001), *Building Secure Software*, Addison-Wesley, Boston.

Washkuch, F. (2006), *Web Fraud Cost More Than $200 Million in 2006*, Available at : http://scmagazine.com/us/news/article/645020/fbi-web-fraud-cost-200-million-2006/ (2007)

White, H.; and Nteli, F. (2004), Internet Banking in the UK : Why Are There not more customers? *Journal of Financial Services Marketing*, 9 (1), 49-56.

Young T. (2006), Cost of ID fraud could reach £3.8bn in four years, Available at : http://www.vnunet.com/computing/news/2168208/cost-id-fraud-reach-8bn-four

Yousafzai, S.; Pallister, J.; and Foxall G. (2003), A Proposed Model of e-trust for Electronic Banking Technovation, 847–860, Available at www.elsevier.com/locate/technovation,

Yousafzai, S.; Pallister, J.; and Foxall, G. (2009), Multi-dimensional Role of Trust in Internet Banking Adoption, *The Service Industries Journal*, Vol. 29, No. 5, May 2009, 591–605.