International Journal of Advanced Research in Management and Social Sciences
ISSN: 2278-6236
Impact Factor: 4.400

RISK OF UNAUTHORIZED SYSTEM ACCESS IN E-BANKING IN INDIA

Prof. S. Singh*

Abstract: *This paper analyzed the bankers' viewpoint towards the factors responsible for risk of unauthorized system access in e-banking in India, its potential impacts and the risk management measures taken by selected public, private and foreign banks. A sample of 107, 104 and 100 respondents is taken for data collection from the different branches located in Haryana, Punjab, Chandigarh and Delhi from selected public, private and foreign banks respectively. Statistical techniques such as mean, mode, standard deviation have been used for the analysis of data. ANOVA technique has been applied to validate the results. The analysis shows that entry of hackers into the system is found as the most important factor leading to the risk of unauthorized system access in the selected banks followed by the interception of confidential information and virus injected into the bank's system in public sector banks; and virus injected into the bank's system and interception of confidential information in private sector banks; and interception of confidential information and information access by unauthorized third party in foreign banks. Further, the loss of data is found as the most potential impact on public and private sector banks followed by theft or tempering with customers' information; whereas theft or tempering with customers' information is found as the most potential impact on foreign banks followed by the disability of bank's internal computer system. However, firewalls is considered as the most adopting risk management measure in public and private sector banks followed by password management, whereas proper authorization of end users is found as the most adopting measure in foreign banks followed by firewalls and password management.*

Key words: *Hackers, Interception, Tempering, Firewalls, Password.*

***Department of Business Administration, Chaudhary Devi Lal University, Sirsa, Haryana, India

Indian banking industry today is in the mid of an IT revolution. New private sector banks and foreign banks have an edge over public sector banks in the implementation of technological solutions. However, public sector banks are in the process of making huge investment in technology. To be successful in this competitive environment, these banks have to take certain steps like cost reduction by economies of scale, better relations with the customers by providing better services and facilities to them. Pressure of performance and profitability will keep them on their toes all the times as the shareholders expect good performance along with good returns on their equity. The changing scenario and the new technologies like internet banking, mobile banking, improvement in payment technology, etc. can help in increasing the scale of economies in providing financial services. With the help of technology, the banks are now able to offer such products and services, which were difficult or impossible with traditional banking. But Indian banks have to go a long way before making themselves technology savvy. India has been able to take one step in this direction - physical cash has been replaced by anytime, anywhere money, but these are more pronounced in foreign and private sector banks. The public sector banks are far behind in technology integration. Thus, there is a huge scope for automation in the banking industry. The service based areas of banks have perhaps been the largest beneficiary of e-banking. ATMs, credit cards, internet banking, mobile banking which are already widely used around the world, have yet to reach their full potential in India. These services and products are all expected to grow in the coming years. No doubt, e-banking provides so many benefits, but face to face contact between the bank and the customer is absent in e-banking transactions, which causes most of the problems like credit card frauds, fraud of internet, etc. Rising competition is forcing the banks to find innovative ways to reduce the cost of transactions and increase the profitability. Technology has been one of the major enabling factors for enhancing the customer convenience in the products and services offered by the various banks and help in enhancing service range but the security of the transactions is a major concern. While it mitigates some risks, but induces some risks also. The main risks of e-banking are: strategic risk, business risk, operational risk, security risk, privacy/security risk, legal risk, cross-border risk, reputational risk, liquidity risk, etc. These risks are highly interdependent and events that affect one area of risk can have ramifications for a range of other risk categories.

REVIEW OF LITERATURE

Various articles appeared in different journals in varied aspects of e-banking, which are restrictive in nature and do not give a comprehensive picture. Ahmad et. al. (2010) discussed the security issues on banking systems and stated that banking system intrusion shows the vulnerabilities that exists in financial institution, that have been used by those illegal and unauthorized individuals or groups to intrude an area with secure environment. With the developing of high technology and information system around the world, banking system should not be left behind in terms of security system and should keep a sharp eye when there is any vulnerability in authentication and authorization that may lead to confidentiality, availability and integrity issues. Fatima (2011) concluded that biometric based authentication and identification systems are the new solutions to address the issues of security and privacy. One thing that can be said with certainty about the future of the biometrics industry is that is growing. Biometrics are finding their way into all kinds of applications beyond access control. It is expected that more and more information systems/computer networks will be secured with biometrics with the rapid expansion of internet and intranet. Adewuyi (2011) examined the concept of information technology, meaning of e-banking, origin of e-banking in Nigeria, areas of information and communication technology deployment by banks, guidelines on e-banking in Nigeria, reasons for automation of banking operation, challenges of regulatory on e-banking in Nigeria and the way forward. It is concluded that the adoption of TCT has influenced the content and quality of banking operations and presents great potential for business re-engineering of Nigerian banks. Thus investment in ICT should form an important component in the overall strategy of banking operation to ensure effective performance. Mermod (2011) analyzed the internet bank branches in Turkey with regard to many dimensions and found that online customers admit that internet bank branches are safe and cheaper and understandable and saving extra time. Internet banking usage rate have increased in the last years, depending on the increase of educated users. The usage rate of the internet banking is significantly related with the education levels. Education and also income level makes an important difference in the usage of internet banking facilities. Karimzadeh and Alam (2012) examined the e-banking challenges in India and concluded that legal and security, socio-cultural and management, banking issues are accepted as challenges for the development of

e-banking. But there is less awareness regarding new technologies and unsuitable software which are ranked respectively as the highest and lowest obstacles in India. Osunmuyiwa (2013) examined the various aspects of online banking risks and the risk management methods employed in mitigating these risks. It is widely recommended that banks that carry out online banking clearly should explain the privacy rule and communicate it to their clients. Banks can also make use of materials like vendor oversight, assignment sheet; excel spreadsheet for risk assessment for policies amongst so many created from a range of date resources to carry out data safekeeping. With this background, an attempt is made to examine the various aspects of risk of unauthorized system access in e-banking in selected banks in India.

SCOPE OF THE STUDY

The present study is confined to the selected public, private and foreign banks in Haryana, Delhi, Chandigarh and Punjab.

OBJECTIVES OF THE STUDY

The present study is conducted to achieve the following objectives of the study:

1. To identify the factors leading to risk of unauthorized system access in e-banking.
2. To analyze the potential impacts of risk of unauthorized system access in e-banking.
3. To appraise the risk management measures for overcoming the risk of unauthorized system access in e-banking.

RESEARCH HYPOTHESES

The following hypotheses have been formulated and tested to validate the results of the study:

H_{01}: There is no significant difference among the bankers' viewpoint towards the factors leading to risk of unauthorized system access in e-banking.

H_{02}: There is no significant difference among the bankers' viewpoint towards the potential impacts of risk of unauthorized system access in e-banking.

H_{03}: There is no significant difference among the bankers' viewpoint towards the risk management measures to overcome the risk of unauthorized system access in e-banking.

SAMPLE PROFILE

For the purpose of the study, all the banks have been divided into three categories *i.e.* public, private and foreign banks. The banks selected from the public sector are State Bank of India (SBI), State Bank of Patiala (SBP), State Bank of Bikaner and Jaipur (SBBJ), Punjab National Bank (PNB), Dena Bank (DB), Oriental Bank of Commerce (OBC), Canara Bank (CB), Central Bank of India (CBI), Union Bank (UB), Corporation Bank (CB), Bank of Baroda (BOB), Allahabad Bank (AB), Bank of India (BOI), Syndicate Bank (SB) and Indian Bank (IB). The banks selected from the private sector are ICICI Bank (ICICI), Axis Bank (AXIS), IDBI Bank (IDBI), HDFC Bank (HDBC), Yes Bank (YB), Kotak Mahindra Bank (KOTAK) and The Federal Bank Limited (FBL). Foreign banks include Standard Chartered Bank, City Bank, SBER Bank, State Bank of Mauritius, ABN-AMRO Bank N.V., HSBC Bank, American Express, BNP Paribas, Deutsche Bank and Barclays Bank.

DATA COLLECTION

The present study is of analytical and exploratory in nature. Accordingly, the use is made of primary as well as secondary data. The primary data were collected with the help of pre-tested structured questionnaire from the respondents (banks' officials) of selected banks on five point Likert Scale *i.e.* Strongly Disagree (SD), Disagree (A), Neutral (N), Agree (A), and Strongly Agree (SA). A sample of 375 respondents is taken from the various branches of the selected banks (125 respondents from each group). After examination, 107 questionnaires from public sector banks, 104 from private sector banks and 100 from foreign banks were found complete and used for further analysis. Besides questionnaires, interviews and discussion techniques were also used to unveil the information. On the other hand, the secondary data were collected mainly from RBI Monthly Bulletins, IBA Bulletins, Economic and Political Weekly, Bank Management, Professional Banker; and newspapers like The Economic Times, The Financial Express and The Hindu were also referred.

DATA ANALYSIS

The collected data were analyzed through descriptive statistical techniques like frequency distribution, percentage, mean, mode, standard deviation. For coding and analyzing the data, weights are assigned in order of importance i.e. 1 to Strongly Disagree (SD), 2 to Disagree (A), 3 to Neutral, 4 to Agree (A), and 5 to Strongly Agree (SA). To examine the bankers' viewpoints towards factors responsible for e-banking risks, their potential impacts,

and the risk management measures taken by the selected banks; ANOVA technique was employed to test the hypotheses and validate the results. The analysis is in conformity with the objectives of the study and the hypotheses formulated. The collected data are analyzed through PASW 18.0 version.

RESULTS AND DISCUSSIONS

(A) Factors Leading to Unauthorized System Access

Table 1 (a) and 1 (b) show the various factors leading to the risk of unauthorized system access in selected banks in India.

Public Sector Banks

Most of the respondents *i.e.* 49 respondents (45.8 per cent) put the entry of hackers into the system (Mean = 4.09, S.D. = 1.060) at the top as the most important factor leading to the unauthorized system access. The interception of confidential information (Mean = 3.77, S.D. = 0.907) is viewed as the second important factor as per the opinion of 63 respondents (58.9 per cent) by the employees of these banks. Virus injected into the bank's system (Mean = 3.76, S.D. = 1.026) is considered as the third most important factor which leads to the unauthorized system access by 45 respondents (42.1 per cent). Information access by unauthorized third party (Mean = 3.61, S.D. = 0.909) is considered as the least important factor by 52 respondents (48.6 per cent), which leads to the unauthorized system access.

Table 1 (a): Factors Leading to Risk of Unauthorized System Access

Statements	N/P	Public Sector Banks					Private Sector Banks					Foreign Banks				
		SD	D	I	A	SA	SD	D	I	A	SA	SD	D	I	A	SA
Entry of Hackers into the System	N	3	7	16	32	49	4	3	37	32	28	5	3	10	47	35
	%	2.8	6.5	15.0	29.9	45.8	3.8	2.9	35.6	30.8	26.9	5.0	3.0	10.0	47.0	35.0
Interception of Confidential Information	N	5	3	20	63	16	2	4	35	52	11	3	6	13	54	24
	%	4.7	2.8	18.7	58.9	15.0	1.9	3.8	33.7	50.0	10.6	3.0	6.0	13.0	54.0	24.0
Information access by unauthorized third party	N	2	11	28	52	14	4	10	43	31	16	5	9	25	44	17
	%	1.9	10.3	26.2	48.6	13.1	3.8	9.6	41.3	29.8	15.4	5.0	9.0	25.0	44.0	17.0
Virus injected into the bank's system	N	4	8	24	45	26	5	3	29	48	19	7	16	17	47	13
	%	3.7	7.5	22.4	42.1	24.3	4.8	2.9	27.9	46.2	18.3	7.0	16.0	17.0	47.0	13.0

Note: N/P Number of Respondents/Percent

Source: Survey

Table 1 (b): Factors Leading to Risk of Unauthorized System Access

Particulars	Public Sector Banks			Private Sector Banks			Foreign Banks			ANOVA	
	N	Mean	S.D.	N	Mean	S.D.	N	Mean	S.D.	F (df=2,308)	Sig.
Entry of Hackers into the System	107	4.09	1.06	104	3.74	1.014	100	4.04	1.014	3.562	.030*
Interception of Confidential Information	107	3.77	0.907	104	3.63	0.801	100	3.9	0.937	2.301	.102
Information access by unauthorized third party	107	3.61	0.909	104	3.43	0.993	100	3.59	1.036	1.007	.366
Virus injected into the bank's system	107	3.76	1.026	104	3.7	0.964	100	3.43	1.121	2.904	.056

Note: N = Number of Respondents, S.D. = Standard Deviation, * Significant at 0.05 level of significance

Source: Survey

Private Sector Banks

Most of the respondents put the entry of hackers into the system (Mean = 3.74, S.D. = 1.014) at the top which leads to the unauthorized system access in these banks. Virus injected into the bank's system (Mean = 3.70, S.D. = 0.964) is viewed as the second important factor by 48 respondents (46.2 per cent). On the other hand, interception of confidential information (Mean = 3.63, S.D. = 0.801) is found as the third most important factor as per the opinion of 52 respondents (50.0 per cent), whereas the information access by unauthorized third party (Mean = 3.43, S.D. = 0.993) is considered as the least important factor by 43 respondents (41.3 per cent).

Foreign Banks

Most of the respondents *i.e.* 47 respondents (47.0 per cent) put the entry of hackers into the system (Mean = 4.04, S.D. = 1.014) at the top and considered it as the most important factor which leads to the unauthorized system access. Interception of confidential information (Mean = 3.90, S.D. = 0.937) is found as the second important factor by 54 respondents (54.0 per cent). On the other hand, information access by unauthorized third party (Mean = 3.59, S.D. = 1.036) is considered by the respondents as the third most important factor by 44 respondents (44.0 per cent), whereas the virus injected into the bank's system (Mean = 3.43, S.D. = 1.121) is considered as the fourth important factor by 47 respondents (47.0 per cent).

The results of ANOVA in Table 1 (b) shows that there is a significant difference among the bankers' viewpoint towards the entry of hackers into the system (p=0.30, df=2, 308) at 0.05 level of significance. Therefore, the null hypothesis (H_{01}) is rejected.

(B) Potential impacts of Unauthorized System Access

Table 2 (a) and 2 (b) exhibit the potential impacts of risk of unauthorized system access on the selected banks.

Public Sector Banks

Loss of data (Mean = 4.22, S.D. = 0.914) is found as the most potential impact on public sector banks as per the opinion of 48 respondents (44.9 per cent). Theft or tempering with customers' information (Mean = 3.93, S.D. = 0.918) is considered by the 51 respondents (47.7 per cent) as the next potential impact on these banks. On the other hand, potential adverse publicity (Mean = 3.79, S.D. = 0.962) is found by the 49 respondents (45.8 per cent) as the third important effect, whereas the disability of bank's internal computer system (Mean = 3.66, S.D. = 0.951) is considered as the next potential impact as per the responses of 45 respondents (42.1 per cent). However, the costs associated with repairing system (Mean = 3.61, S.D. = 0.898) is found as the next potential impact on public sector banks by 54 respondents (50.5 per cent).

Table 2 (a): Potential Impacts of Risk of Unauthorized System Access on Banks

Statements	N/P	Public Sector Banks					Private Sector Banks					Foreign Banks				
		SD	D	I	A	SA	SD	D	I	A	SA	SD	D	I	A	SA
Loss of data	N	3	2	11	43	48	7	0	9	53	35	7	12	24	38	19
	%	2.8	1.9	10.3	40.2	44.9	6.7	0	8.7	51.0	33.7	7.0	12.0	24.0	38.0	19.0
Theft or tempering with customers' information	N	2	6	19	51	29	4	4	29	45	22	4	8	23	47	18
	%	1.9	5.6	17.8	47.7	27.1	3.8	3.8	27.9	43.3	21.2	4.0	8.0	23.0	47.0	18.0
Disability of bank's internal computer system	N	2	10	30	45	20	4	2	34	59	5	3	11	22	50	14
	%	1.9	9.3	28.0	42.1	18.7	3.8	1.9	32.7	56.7	4.8	3.0	11.0	22.0	50.0	14.0
Costs associated with repairing system	N	5	3	33	54	12	2	8	24	60	10	7	11	22	50	10
	%	4.7	2.8	30.8	50.5	11.2	1.9	7.7	23.1	57.7	9.6	7.0	11.0	22.0	50.0	10.0
Potential adverse	N	3	7	24	49	24	5	3	34	48	14	5	11	20	48	16

publicity	%	2.8	6.5	22.4	45.8	22.4	4.8	2.9	32.7	46.2	13.5	5.0	11.0	20.0	48.0	16.0

Note: N/P = Number of Respondents/Percent

Source: Survey

Table 2 (b): Potential Impacts of Risk of Unauthorized System Access on Banks

Particulars	Public Sector Banks			Private Sector Banks			Foreign Banks			ANOVA	
	N	Mean	S.D.	N	Mean	S.D.	N	Mean	S.D.	F (df=2,308)	Sig.
Loss of data	107	4.22	0.914	104	4.05	1.018	100	3.5	1.142	13.866	.000*
Theft or tempering with customers' information	107	3.93	0.918	104	3.74	0.965	100	3.67	0.995	1.972	.141
Disability of bank's internal computer system	107	3.66	0.951	104	3.57	0.785	100	3.61	0.963	.301	.740
Costs associated with repairing system	107	3.61	0.898	104	3.65	0.833	100	3.45	1.048	1.344	.262
Potential adverse publicity	107	3.79	0.962	104	3.61	0.929	100	3.59	1.045	1.288	.277

Note: N = Number of Respondents, S.D. = Standard Deviation, * Significant at 0.05 level of significance

Source: Survey

Private Sector Banks

Loss of data (Mean = 4.05, S.D. = 1.018) is found by the 53 respondents (51.0 per cent) as the most potential impact on private sector banks. Theft or tempering with customers' information (Mean = 3.74, S.D. = 0.965) is considered the next potential impact as viewed by 45 respondents (43.3 per cent). On the other hand, costs associated with repairing system (Mean = 3.65, S.D. = 0.833) is viewed as next potential impact by 60 respondents (57.7 per cent), whereas the potential adverse publicity (Mean = 3.61, S.D. = 0.929) is considered by the 48 respondents (46.2 per cent) as next potential impact on these banks. However, the disability of bank's internal computer system (Mean = 3.57, S.D. = 0.785) is considered as the least potential impact by 59 respondents (56.7 per cent) as given in Table 2 (a).

Foreign Banks

Theft or tempering with customers' information (Mean = 3.67, S.D. = 0.995) is found as the most potential impact on these banks by 47 respondents (47.0 per cent). The disability of bank's internal computer system (Mean = 3.61, S.D. = 0.963) is considered as the next potential impact by the 50 respondents (50.0 per cent) on foreign banks. Potential adverse publicity (Mean = 3.59, S.D. = 1.045) is found as the third important impact by 48 respondents (48.0 per cent). Loss of data (Mean = 3.50, S.D. = 1.142) is considered by the respondents as the next potential impact as viewed by 38 respondents (38.0 per cent).

However, 50 respondents (50.0 per cent) are of the opinion that the costs associated with repairing the system (Mean = 3.45, S.D. = 1.048) is the least potential impact on these banks.

The results of ANOVA in Table 2 (b) show that there is a significant difference among the bankers' viewpoint towards the loss of data (p=0.00, df=2, 308) at 0.05 level of significance. Therefore, the null hypothesis (H_{02}) is rejected.

(C) Risk Management Measures to Overcome Unauthorized System Access

Various risk management measures to overcome the risk of unauthorized system access are given in Table 3 (a) and 3 (b).

Public Sector Banks

Firewalls (Mean = 4.49, S.D. = 0.757) is put at the top by 65 respondents (60.7 per cent) as the most adopting risk management measure in these banks. Password management (Mean = 4.44, S.D. = 0.791) is considered as the next most adopting measure by 62 respondents (57.9 per cent). On the other hand, the encryption techniques (Mean = 4.31, S.D. = 0.936) is considered as the third important measure by 57 respondents (53.3 per cent), whereas the proper authorization of end users (Mean = 4.15, S.D. = 0.684) is considered as next adopting measure as viewed by 64 respondents (59.8 per cent). However, penetration testing for vulnerabilities (Mean = 4.14, S.D. = 0.806) and surveillance to detect anomalies in usage (Mean = 4.00, S.D. = 0.789) are considered as the least adopting measures by 56 respondents (52.3 per cent) and 61 respondent (57.0 per cent) respectively in these banks.

Table 3 (a): Risk Management Measures to Overcome the Risk of Unauthorized System Access

Statements	N/P	Public Sector Banks					Private Sector Banks					Foreign Banks				
		SD	D	I	A	SA	SD	D	I	A	SA	SD	D	I	A	SA
Penetration testing for vulnerabilities	N	1	4	10	56	36	1	1	9	57	36	1	3	22	53	21
	%	.9	3.7	9.3	52.3	33.6	1.0	1.0	8.7	54.8	34.6	1.0	3.0	22.0	53.0	21.0
Surveillance to detect anomalies in usage	N	1	4	15	61	26	2	3	12	45	42	3	12	13	51	21
	%	.9	3.7	14.0	57.0	24.3	1.9	2.9	11.5	43.3	40.4	3.0	12.0	13.0	51.0	21.0
Proper authorization of end users	N	0	3	9	64	31	0	1	10	62	31	1	3	10	48	38
	%	0	2.8	8.4	59.8	29.0	0	1.0	9.6	59.6	29.8	1.0	3.0	10.0	48.0	38.0
Firewalls	N	0	4	5	33	65	1	0	4	23	76	3	6	8	59	24
	%	0	3.7	4.7	30.8	60.7	1.0	0	3.8	22.1	73.1	3.0	6.0	8.0	59.0	24.0
Password management	N	1	2	8	34	62	1	1	4	25	73	3	8	10	49	30
	%	.9	1.9	7.5	31.8	57.9	1.0	1.0	3.8	24.0	70.2	3.0	8.0	10.0	49.0	30.0
Encryption techniques	N	3	2	11	34	57	1	0	8	34	61	7	9	6	53	25
	%	2.8	1.9	10.3	31.8	53.3	1.0	0	7.7	32.7	58.7	7.0	9.0	6.0	53.0	25.0

Note: N/P = Number of Respondents/Percent

Source: Survey

Table 3 (b): Risk Management Measures to Overcome the Risk of Unauthorized System Access

Particulars	Public Sector Banks			Private Sector Banks			Foreign Banks			ANOVA	
	N	Mean	S.D.	N	Mean	S.D.	N	Mean	S.D.	F (df=2,308)	Sig.
Penetration testing for vulnerabilities	107	4.14	0.806	104	4.21	0.72	100	3.9	0.798	4.500	.012*
Surveillance to detect anomalies in usage	107	4	0.789	104	4.17	0.886	100	3.75	1.019	5.680	.004*
Proper authorization of end users	107	4.15	0.684	104	4.18	0.635	100	4.19	0.813	.096	.909
Firewalls	107	4.49	0.757	104	4.66	0.648	100	3.95	0.914	23.123	.000*
Password management	107	4.44	0.791	104	4.62	0.701	100	3.95	0.999	17.241	.000*
Encryption techniques	107	4.31	0.936	104	4.48	0.724	100	3.8	1.128	14.370	.000*

Note: N = Number of Respondents, S.D. = Standard Deviation, * Significant at 0.05 level of significance

Source: Survey

Private Sector Banks

Firewalls (Mean = 4.66, S.D. = 0.648) is found as the top most adopting measure in private sector banks by 76 respondents (73.1 per cent). Password management (Mean = 4.62, S.D. = 0.648) is viewed as the next most adopting measure by 73 respondents (70.2 per cent). On the other hand, the encryption techniques (Mean = 4.48, S.D. = 0.724) is considered as the third important measure by the respondents as viewed by 61 respondents (58.7 per cent). Penetration testing for vulnerabilities (Mean = 4.21, S.D. = 0.720) is found as next adopting measure by 57 respondents (54.8 per cent). However, the proper authorization of end users (Mean = 4.18, S.D. = 0.635) and surveillance to detect anomalies in usage (Mean = 4.17, S.D. = 0.886) are considered as the least adopting measures by 62 respondents (59.6 per cent) and 45 respondents (43.3 per cent) respectively in these banks.

Foreign Banks

Proper authorization of end users (Mean = 4.15, S.D. = 0.684) is found as the most adopting measure in these banks by 48 respondents (48.0 per cent). Firewalls (Mean = 3.95, S.D. = 0.914) and password management (Mean = 3.95, S.D. = 0.999) are considered as the next most adopting measures by the respondents in these banks as per the responses given by 59 respondents (59.0 per cent) and 49 respondents (49.0 per cent) respectively. On the other hand, the penetration testing for vulnerabilities (Mean = 3.90, S.D. = 0.798) is

considered as the next adopting measure as viewed by 53 respondents (53.0 per cent), whereas the encryption techniques (Mean = 3.80, S.D. = 1.128) is found less important measure as per the opinion of 53 respondents (53.0 per cent). However, the surveillance to detect anomalies in usage (Mean = 3.75, S.D. = 1.019) is considered by 51 respondents (51.0 per cent) as the least adopting measure in these banks.

The results of ANOVA in Table 3 (b) shows that there is a significant difference among the bankers' viewpoints towards penetration testing for vulnerabilities (p=0.012, df=2, 308), surveillance to detect anomalies in usage (p=0.004), firewalls (p=0.00, df=2, 308), password management (p=0.00, df=2, 308) and encryption techniques (p=0.00, df=2, 308) at 0.05 level of significance. Therefore, the null hypothesis (H_{03}) is rejected.

CONCLUSION

To sum up, the entry of hackers into the system is found as the most important factor leading to the risk of unauthorized system access in the selected banks followed by the interception of confidential information and virus injected into the bank's system in public sector banks; and virus injected into the bank's system and interception of confidential information in private sector banks; interception of confidential information and information access by unauthorized third party in foreign banks. Further, the loss of data is found as the most potential impact on public and private sector banks followed by theft or tempering with customers' information; whereas theft or tempering with customers' information is found as the most potential impact on foreign banks followed by the disability of bank's internal computer system. However, firewalls is considered as the most adopting risk management measure in public and private sector banks followed by password management, whereas proper authorization of end users is found as the most adopting measure in foreign banks followed by firewalls and password management.

REFERENCES

1. Adewuyi, I. D. (2011), Electronic Banking in Nigeria: Challenges of the Regulatory Authorities and the Way Forward", *International Journal of Economic Development Research and Investment,* Vol. 2, No. 01, April, pp. 149-156
2. Ahmad, Mohd. Khairul Affendy and others (2010), "Security Issues on Banking Systems", *International Journal of Computer Science and Information Technologies*, Vol. 1(4), pp. 268-272, ISSN: 0975-9646

3. Fatima, Amtul (2011), "E-Banking Security Issues - Is There A Solution in Biometrics?", Journal of Internet Banking and Commerce, August, Vol. 16, No. 02, pp. 1-9.
4. Karimzadeh, Majid and Alam, Dastgir (2012), "Electronic Banking Challenges in India: An Empirical Investigation", *Interdisciplinary Journal of Contemporary Research in Business",* Vol. 04, No. 02, June, pp. 31-45.
5. Mermod, Asli Yijksel (2011), "Customer's Perspectives and Risk Issues on E-Banking in Turkey: Should We Still be Online?", *Journal of Internet Banking and Commerce,* Vol. 16, No. 01, pp. 1-15
6. Osunmuyiwa, Olufolabi (2013), "Online Banking and the Risks Involved", *Research Journal of Information Technology,* 5 (2), 50-54, ISSN: 2041-3106, e-ISSN: 2041-3114.